INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

January 2026

The total zero-day vulnerabilities count for January month: 770

Command Injection	SQL Injection	SSRF	Code Injection	Cross-Site Scripting	Malicious File Upload	Path Traversal
65	153	14	16	497	18	7

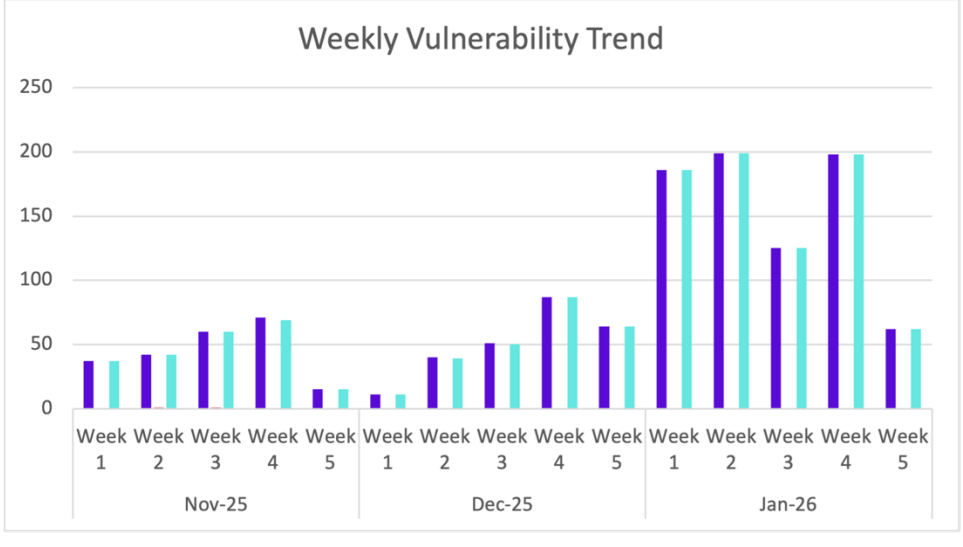
Zero-day vulnerabilities protected through core rules	770
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	770

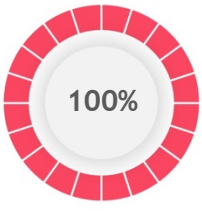
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

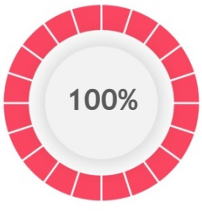
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



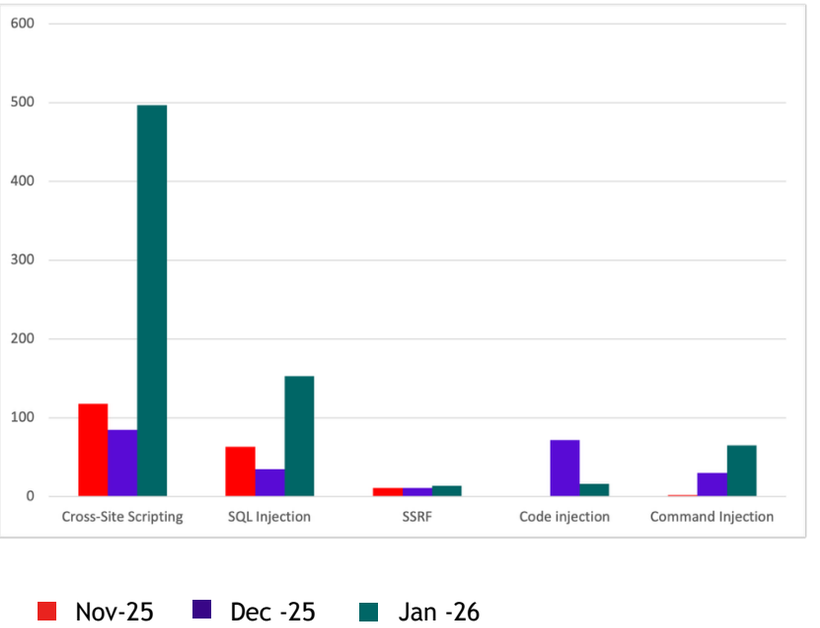


of the zero-day vulnerabilities were protected by the core rules in the last month



of the zero-day vulnerabilities were reported by Indusface Scanner in the last month

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-47903	LiteSpeed Web Server Enterprise - authenticated command injection in the external app configuration interface	LiteSpeed Web Server Enterprise 5.4.11 contains an authenticated command injection vulnerability in the external app configuration interface. Authenticated administrators can inject shell commands through the 'Command' parameter in the server configuration, allowing remote code execution via path traversal and bash command injection.	Patched by core rule	Y
CVE-2021-47891	Unified Remote 3	Unified Remote 3.9.0.2463 contains a remote code execution vulnerability that allows attackers to send crafted network packets to execute arbitrary commands. Attackers can exploit the service by connecting to port 9512 and sending specially crafted packets to open a command prompt and download and execute malicious payloads.	Patched by core rule	Y
CVE-2026-1326	A weakness has been identified in Totolink	A weakness has been identified in Totolink	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	NR1800X 9	NR1800X 9.1.0u.6279_B20210910. This vulnerability affects the function setWanCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. This manipulation of the argument Hostname causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.		
CVE-2026-1324	A vulnerability was identified in Sangfor Operation and Maintenance Management System up to 3	A vulnerability was identified in Sangfor Operation and Maintenance Management System up to 3.0.12. Affected by this issue is the function SessionController of the file /isomp-protocol/protocol/session of the component SSH Protocol Handler. The manipulation of the argument keypassword leads to os command injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2021-47863	MacPaw Encrypto - unquoted service path in its Encrypto Service configuration	MacPaw Encrypto 1.0.1 contains an unquoted service path vulnerability in its Encrypto Service configuration that allows local attackers to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files\Encrypto\ to inject malicious executables and escalate privileges on Windows systems.	Patched by core rule	Y
CVE-2021-47851	Mini Mouse 9	Mini Mouse 9.2.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary commands through an unauthenticated HTTP endpoint. Attackers can leverage the /op=command endpoint to download and execute payloads by sending crafted JSON requests with malicious script commands.	Patched by core rule	Y
CVE-2021-47748	Hasura GraphQL 1	Hasura GraphQL 1.3.3 contains a remote code execution vulnerability that allows attackers to execute arbitrary shell commands	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through SQL query manipulation. Attackers can inject commands into the run_sql endpoint by crafting malicious GraphQL queries that execute system commands through PostgreSQL's COPY FROM PROGRAM functionality.		
CVE-2026-1150	A security flaw has been discovered in Totolink LR350 9	A security flaw has been discovered in Totolink LR350 9.3.5u.6369_B20220309. Impacted is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument command results in command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-1149	A vulnerability was identified in Totolink LR350 9	A vulnerability was identified in Totolink LR350 9.3.5u.6369_B20220309. This issue affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. The manipulation of the argument ip leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-1125	A weakness has been identified in D-Link DIR-823X 250416	A weakness has been identified in D-Link DIR-823X 250416. Affected by this issue is the function sub_412E7C of the file /goform/set_wifidog_settings. Executing a manipulation of the argument wd_enable can lead to command injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2021-47816	Thecus N4800Eco NAS Server Control Panel contains a command injection vulnerability that allows authenticated attackers to execute arbitr...	Thecus N4800Eco NAS Server Control Panel contains a command injection vulnerability that allows authenticated attackers to execute arbitrary system commands through user management endpoints. Attackers can inject commands via username and batch user creation parameters to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execute shell commands with administrative privileges.		
CVE-2021-47794	ZesleCP 3	ZesleCP 3.1.9 contains an authenticated remote code execution vulnerability that allows attackers to create malicious FTP accounts with shell injection payloads. Attackers can exploit the FTP account creation endpoint by injecting a reverse shell command that establishes a network connection to a specified listening host.	Patched by core rule	Y
CVE-2026-22864	Deno is a JavaScript, TypeScript, and WebAssembly runtime	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Before 2.5.6, a prior patch aimed to block spawning Windows batch/shell files by returning an error when a spawned pathâ€™s extension matched .bat or .cmd. That check performs a case-sensitive comparison against lowercase literals and therefore can be bypassed when the extension uses alternate casing (for example .BAT, .Bat, etc.). This vulnerability is fixed in 2.5.6.	Patched by core rule	Y
CVE-2023-54339	Webgrind 1	Webgrind 1.1 contains a remote command execution vulnerability that allows unauthenticated attackers to inject OS commands via the dataFile parameter in index.php. Attackers can execute arbitrary system commands by manipulating the dataFile parameter, such as using payload '0%27%26calc.exe%26%27' to execute commands on the target system.	Patched by core rule	Y
CVE-2022-50919	Tdarr - unauthenticated remote code execution in its Help terminal	Tdarr 2.00.15 contains an unauthenticated remote code execution vulnerability in its Help terminal that allows attackers to inject and chain arbitrary commands. Attackers can exploit the lack of input filtering by chaining commands like `--help; curl .py | python` to execute remote code without authentication.	Patched by core rule	Y
CVE-2022-50909	Algo - command injection in the fm-data	Algo 8028 Control Panel version 3.3.3 contains a command injection vulnerability in the fm-data.lua endpoint that	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows authenticated attackers to execute arbitrary commands. Attackers can exploit the insecure 'source' parameter by injecting commands that are executed with root privileges, enabling remote code execution through a crafted POST request.		
CVE-2025-64155	An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSIEM 7	An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4, FortiSIEM 7.1.0 through 7.1.8, FortiSIEM 7.0.0 through 7.0.4, FortiSIEM 6.7.0 through 6.7.10 may allow an attacker to execute unauthorized code or commands via crafted TCP requests.	Patched by core rule	Y
CVE-2025-15502	A vulnerability was identified in Sangfor Operation and Maintenance Management System up to 3	A vulnerability was identified in Sangfor Operation and Maintenance Management System up to 3.0.8. The affected element is the function SessionController of the file /isomp-protocol/protocol/session. Such manipulation of the argument Hostname leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-22688	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.5, there is a command injection vulnerability that allows authenticated users to inject stdio_config.command/args into MCP stdio settings, causing the server to execute subprocesses using these injected values. This issue has been patched in version 0.2.5.	Patched by core rule	Y
CVE-2025-15501	A vulnerability was determined in Sangfor Operation and Maintenance Management System up to 3	A vulnerability was determined in Sangfor Operation and Maintenance Management System up to 3.0.8. Impacted is the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		WriterHandle.getCmd of the file /isomp-protocol/protocol/getCmd. This manipulation of the argument sessionPath causes os command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-15500	A vulnerability was found in Sangfor Operation and Maintenance Management System up to 3	A vulnerability was found in Sangfor Operation and Maintenance Management System up to 3.0.8. This issue affects some unknown processing of the file /isomp-protocol/protocol/getHis of the component HTTP POST Request Handler. The manipulation of the argument sessionPath results in os command injection. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15499	A vulnerability has been found in Sangfor Operation and Maintenance Management System up to 3	A vulnerability has been found in Sangfor Operation and Maintenance Management System up to 3.0.8. This vulnerability affects the function uploadCN of the file VersionController.java. The manipulation of the argument filename leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-70161	EDIMAX BR-6208AC V2_1	EDIMAX BR-6208AC V2_1.02 is vulnerable to Command Injection. This arises because the pppUserName field is directly passed to a shell command via the system() function without proper sanitization. An attacker can exploit this by injecting malicious commands into the pppUserName field, allowing arbitrary code execution.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-0732	A vulnerability was found in D-Link DI-8200G 17	A vulnerability was found in D-Link DI-8200G 17.12.20A1. This affects an unknown function of the file /upgrade_filter.asp. The manipulation of the argument path results in command injection. The attack may be performed from remote. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-56425	An issue was discovered in the AppConnector component version 10	An issue was discovered in the AppConnector component version 10.10.0.183 and earlier of enaio 10.10, in the AppConnector component version 11.0.0.183 and earlier of enaio 11.0, and in the AppConnctor component version 11.10.0.183 and earlier of enaio 11.10. The vulnerability allows authenticated remote attackers to inject arbitrary SMTP commands via crafted input to the /osrest/api/organization/sendmail endpoint	Patched by core rule	Y
CVE-2025-67089	the `plugins - command injection in the GL-iNet GL-AXT1800 router firmware v4.6.8. The vulnerability is present	A command injection vulnerability exists in the GL-iNet GL-AXT1800 router firmware v4.6.8. The vulnerability is present in the `plugins.install_package` RPC method, which fails to properly sanitize user input in package names. Authenticated attackers can exploit this to execute arbitrary commands with root privileges	Patched by core rule	Y
CVE-2026-22035	Greenshot is an open source Windows screenshot utility	Greenshot is an open source Windows screenshot utility. Versions 1.3.310 and below arvulnerable to OS Command Injection through unsanitized filename processing. The FormatArguments method in ExternalCommandDestination.cs:269 uses string.Format() to insert user-controlled filenames directly into shell commands without sanitization, allowing attackers to execute arbitrary commands by crafting malicious filenames containing shell metacharacters. This issue is fixed in version 1.3.311.	Patched by core rule	Y
CVE-2019-25289	SmartLiving SmartLAN	SmartLiving SmartLAN <=6.x	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	<=6.x - authenticated remote command injection in the web	contains an authenticated remote command injection vulnerability in the web.cgi binary through the 'par' POST parameter with the 'testemail' module. Attackers can exploit the unsanitized parameter and system() function call to execute arbitrary system commands with root privileges using default credentials.	rule	
CVE-2017-20216	FLIR Thermal Camera PT-Series firmware version 8	FLIR Thermal Camera PT-Series firmware version 8.0.0.64 contains multiple unauthenticated remote command injection vulnerabilities in the controllerFlirSystem.php script. Attackers can execute arbitrary system commands as root by exploiting unsanitized POST parameters in the execFlirSystem() function through shell_exec() calls. Exploitation evidence was observed by the Shadowserver Foundation on 2026-01-06 (UTC).	Patched by core rule	Y
CVE-2017-20215	FLIR Thermal Camera FC-S/PT firmware version 8	FLIR Thermal Camera FC-S/PT firmware version 8.0.0.64 contains an authenticated OS command injection vulnerability that allows attackers to execute shell commands with root privileges. Authenticated attackers can inject arbitrary shell commands through unvalidated input parameters to gain complete control of the thermal camera system.	Patched by core rule	Y
CVE-2025-69262	pnpm is a package manager	pnpm is a package manager. Versions 6.25.0 through 10.26.2 have a Command Injection vulnerability when using environment variable substitution in .npmrc configuration files with tokenHelper settings. An attacker who can control environment variables during pnpm operations could achieve Remote Code Execution (RCE) in build environments. This issue is fixed in version 10.27.0.	Patched by core rule	Y
CVE-2025-61492	A command injection vulnerability in the execute_command function of terminal-controller-mcp 0	A command injection vulnerability in the execute_command function of terminal-controller-mcp 0.1.7 allows attackers to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execute arbitrary commands via a crafted input.		
CVE-2025-61489	A command injection vulnerability in the shell_exec function of sonirico mcp-shell v0	A command injection vulnerability in the shell_exec function of sonirico mcp-shell v0.3.1 allows attackers to execute arbitrary commands via supplying a crafted command string.	Patched by core rule	Y
CVE-2025-15472	A flaw has been found in TRENDnet TEW-811DRU 1	A flaw has been found in TRENDnet TEW-811DRU 1.0.2.0. This affects the function setDeviceURL of the file uapply.cgi of the component httpd . This manipulation of the argument DeviceURL causes os command injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-0641	A security vulnerability has been detected in TOTOLINK WA300 5	A security vulnerability has been detected in TOTOLINK WA300 5.2cu.7112_B20190227. This vulnerability affects the function sub_401510 of the file cstecgi.cgi. The manipulation of the argument UPLOAD_FILENAME leads to command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2020-36910	Cayin Signage Media Player - authenticated remote command injection in system	Cayin Signage Media Player 3.0 contains an authenticated remote command injection vulnerability in system.cgi and wizard_system.cgi pages. Attackers can exploit the 'NTP_Server_IP' parameter with default credentials to execute arbitrary shell commands as root.	Patched by core rule	Y
CVE-2025-64424	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. In Coolify versions up to and including v4.0.0-beta.434, a command injection vulnerability exists in the git source input fields of a resource, allowing a low privileged user (member) to execute system commands	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as root on the Coolify instance. As of time of publication, it is unclear if a patch is available.		
CVE-2025-64419	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.445, parameters coming from docker-compose.yaml are not sanitized when used in commands. If a victim user creates an application from an attacker repository (using build pack "docker compose"), the attacker can execute commands on the Coolify instance as root. Version 4.0.0-beta.445 fixes the issue.	Patched by core rule	Y
CVE-2025-59157	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.420.7, the Git Repository field during project creation is vulnerable to command injection. User input is not properly sanitized, allowing attackers to inject arbitrary shell commands that execute on the underlying server during the deployment workflow. A regular member user can exploit this vulnerability. Version 4.0.0-beta.420.7 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-59156	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to version 4.0.0-beta.420.7, a Remote Code Execution (RCE)*vulnerability exists in Coolify's application deployment workflow. This flaw allows a low-privileged member to inject arbitrary Docker Compose directives during project creation or updates. By defining a malicious service that mounts the host filesystem, an attacker can achieve root-level command execution on the host OS, completely bypassing container isolation. Version 4.0.0-beta.420.7 contains a patch	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		for the issue.		
CVE-2025-66398	Signal K Server is a server application that runs on a central hub in a boat	Signal K Server is a server application that runs on a central hub in a boat. Prior to version 2.19.0, an unauthenticated attacker can pollute the internal state (`restoreFilePath`) of the server via the `/skServer/validateBackup` endpoint. This allows the attacker to hijack the administrator's "Restore" functionality to overwrite critical server configuration files (e.g., `security.json`, `package.json`), leading to account takeover and Remote Code Execution (RCE). Version 2.19.0 patches this vulnerability.	Patched by core rule	Y
CVE-2025-68700	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In versions prior to 0.23.0, a low-privileged authenticated user (normal login account) can execute arbitrary system commands on the server host process via the frontend Canvas CodeExec component, completely bypassing sandbox isolation. This occurs because untrusted data (stdout) is parsed using eval() with no filtering or sandboxing. The intended design was to "automatically convert string results into Python objects," but this effectively executes attacker-controlled code. Additional endpoints lack access control or contain inverted permission logic, significantly expanding the attack surface and enabling chained exploitation. Version 0.23.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2015-10145	Gargoyle router management utility - authenticated OS command execution in /utility/run_commands	Gargoyle router management utility versions 1.5.x contain an authenticated OS command execution vulnerability in /utility/run_commands.sh. The application fails to properly restrict or validate input supplied via the 'commands' parameter, allowing an authenticated attacker to execute arbitrary shell commands on the underlying system. Successful exploitation may result in full compromise of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the device, including unauthorized access to system files and execution of attacker-controlled commands.		
CVE-2021-47747	meterN - authenticated remote code execution in admin_meter2	meterN 1.2.3 contains an authenticated remote code execution vulnerability in admin_meter2.php and admin_indicator2.php scripts. Attackers can exploit the 'COMMANDx' and 'LIVECOMMANDx' POST parameters to execute arbitrary system commands with administrative privileges.	Patched by core rule	Y
CVE-2021-47745	Cypress Solutions CTM-200 - authenticated command injection in the firmware upgrade script	Cypress Solutions CTM-200 2.7.1 contains an authenticated command injection vulnerability in the firmware upgrade script that allows remote attackers to execute shell commands. Attackers can exploit the 'fw_url' parameter in the ctm-config-upgrade.sh script to inject and execute arbitrary commands with root privileges.	Patched by core rule	Y
CVE-2025-15391	A weakness has been identified in D-Link DIR-806A 100CNb11	A weakness has been identified in D-Link DIR-806A 100CNb11. Affected is the function ssdpcgi_main of the component SSDP Request Handler. This manipulation causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2024-58338	Anevia Flamingo XL 3	Anevia Flamingo XL 3.2.9 contains a restricted shell vulnerability that allows remote attackers to escape the sandboxed environment through the traceroute command. Attackers can exploit the traceroute command to inject shell commands and gain full root access to the device by bypassing the restricted login environment.	Patched by core rule	Y
CVE-2022-50795	SOUND4 IMPACT/FIRST/PULSE/Eco <=2	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains a conditional command injection vulnerability that allows local authenticated users to create malicious files in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/tmp directory. Unauthenticated attackers can execute commands by making a single HTTP POST request to the traceroute.php script, which triggers the malicious file and then deletes it after execution.		
CVE-2022-50794	SOUND4 IMPACT/FIRST/PULSE/Eco - unauthenticated command injection in the username parameter	SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated command injection vulnerability in the username parameter. Attackers can exploit index.php and login.php scripts by injecting arbitrary shell commands through the HTTP POST 'username' parameter to execute system commands.	Patched by core rule	Y
CVE-2022-50793	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x - authenticated command injection in the www-data-handler	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains an authenticated command injection vulnerability in the www-data-handler.php script that allows attackers to inject system commands through the 'services' POST parameter. Attackers can exploit this vulnerability by crafting malicious 'services' parameter values to execute arbitrary system commands with www-data user privileges.	Patched by core rule	Y
CVE-2022-50791	SOUND4 IMPACT/FIRST/PULSE/Eco <=2	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains a conditional command injection vulnerability that allows local authenticated users to create malicious files in the /tmp directory. Unauthenticated attackers can execute commands by making a single HTTP POST request to the vulnerable ping.php script, which triggers the malicious file and then deletes it.	Patched by core rule	Y
CVE-2022-50789	SOUND4 IMPACT/FIRST/PULSE/Eco <=2	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains a command injection vulnerability that allows local authenticated users to create malicious files in the /tmp directory with .dns.pid extension. Unauthenticated attackers can execute the malicious commands by making a		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		single HTTP POST request to the vulnerable dns.php script, which triggers command execution and then deletes the file.		
CVE-2022-50691	MiniDVBLinux 5	MiniDVBLinux 5.4 contains a remote command execution vulnerability that allows unauthenticated attackers to execute arbitrary commands as root through the 'command' GET parameter. Attackers can exploit the /tpl/commands.sh endpoint by sending malicious command values to gain root-level system access.	Patched by core rule	Y
CVE-2025-15357	A vulnerability was found in D-Link DI-7400G+ 19	A vulnerability was found in D-Link DI-7400G+ 19.12.25A1. This affects an unknown function of the file /msp_info.htm?flag=cmd. The manipulation of the argument cmd results in command injection. The attack can be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-15256	A vulnerability was identified in Edimax BR-6208AC 1	A vulnerability was identified in Edimax BR-6208AC 1.02/1.03. Affected is the function formStaDrvSetup of the file /goform/formStaDrvSetup of the component Web-based Configuration Interface. The manipulation of the argument rootAPmac leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. Edimax confirms this issue: "The product mentioned, EDIMAX BR-6208AC V2, has reached its End of Life (EOL) status. It is no longer supported or maintained by Edimax, and it is no longer available for purchase in the market. Consequently, there will be no further firmware updates or patches for this device. We recommend users upgrade to newer models for better security." This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-15254	A vulnerability was found in Tenda W6-S 1	A vulnerability was found in Tenda W6-S 1.0.0.4(510). This affects the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		TendaAte of the file /goform/ate of the component ATE Service. Performing manipulation results in os command injection. The attack may be initiated remotely. The exploit has been made public and could be used.		
CVE-2025-15192	A security vulnerability has been detected in D-Link DWR-M920 up to 1	A security vulnerability has been detected in D-Link DWR-M920 up to 1.1.50. The impacted element is the function sub_415328 of the file /boafrm/formLtefotaUpgradeQuectel. Such manipulation of the argument fota_url leads to command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-15191	A weakness has been identified in D-Link DWR-M920 up to 1	A weakness has been identified in D-Link DWR-M920 up to 1.1.50. The affected element is the function sub_4155B4 of the file /boafrm/formLtefotaUpgradeFibocom. This manipulation of the argument fota_url causes command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-15139	A vulnerability has been found in TRENDnet TEW-822DRE 1	A vulnerability has been found in TRENDnet TEW-822DRE 1.00B21/1.01B06. This affects the function sub_43ACF4 of the file /boafrm/formWsc. Such manipulation of the argument peerPin leads to command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15137	A vulnerability was detected in TRENDnet TEW-800MB 1	A vulnerability was detected in TRENDnet TEW-800MB 1.0.1.0. Affected by this vulnerability is the function sub_F934 of the file NTPSyncWithHost.cgi. The manipulation results in command injection. The attack may be launched remotely. The exploit is now public and may be used. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-15136	A security vulnerability has been detected in TRENDnet TEW-800MB 1	A security vulnerability has been detected in TRENDnet TEW-800MB 1.0.1.0. Affected is the function do_setWizard_asp of the file /goform/wizardset of the component Management Interface. The manipulation of the argument WizardConfigured leads to command injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15133	A vulnerability was identified in ZSPACE Z4Pro+ 1	A vulnerability was identified in ZSPACE Z4Pro+ 1.0.0440024. The impacted element is the function zfilev2_api_CloseSafe of the file /v2/file/safe/close of the component HTTP POST Request Handler. Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2025-15132	A vulnerability was determined in ZSPACE Z4Pro+ 1	A vulnerability was determined in ZSPACE Z4Pro+ 1.0.0440024. The affected element is the function zfilev2_api_open of the file /v2/file/safe/open of the component HTTP POST Request Handler. This manipulation causes command injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	Patched by core rule	Y
CVE-2025-15131	A vulnerability was found in ZSPACE Z4Pro+ 1	A vulnerability was found in ZSPACE Z4Pro+ 1.0.0440024. Impacted is the function zfilev2_api_SafeStatus of the file /v2/file/safe/status of the component HTTP POST Request Handler. The manipulation results in command injection. The attack may be performed from remote. The exploit has been made public and could	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be used. The vendor was contacted early about this disclosure.		
CVE-2025-66738	An issue in Yealink T21P_E2 Phone 52	An issue in Yealink T21P_E2 Phone 52.84.0.15 allows a remote normal privileged attacker to execute arbitrary code via a crafted request the ping function of the diagnostic component.	Patched by core rule	Y

Code Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-1327	A security vulnerability has been detected in Totolink NR1800X 9	A security vulnerability has been detected in Totolink NR1800X 9.1.0u.6279_B20210910. This issue affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component POST Request Handler. Such manipulation of the argument command leads to command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2021-47778	GetSimple CMS My SMTP Contact Plugin 1	GetSimple CMS My SMTP Contact Plugin 1.1.2 contains a PHP code injection vulnerability. An authenticated administrator can inject arbitrary PHP code through plugin configuration parameters, leading to remote code execution on the server.	Patched by core rule	Y
CVE-2021-47770	OpenPLC v3 contains an authenticated remote code execution vulnerability that allows attackers with valid credentials to inject malicious...	OpenPLC v3 contains an authenticated remote code execution vulnerability that allows attackers with valid credentials to inject malicious code through the hardware configuration interface. Attackers can upload a custom hardware layer with embedded reverse shell code that establishes a network connection to a specified IP and port, enabling remote command execution.	Patched by core rule	Y
CVE-2026-20045	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Un...	A vulnerability in Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM & Presence Service (Unified CM IM&P), Cisco Unity Connection, and Cisco Webex Calling Dedicated Instance could allow an unauthenticated, remote attacker to execute	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to improper validation of user-supplied input in HTTP requests. An attacker could exploit this vulnerability by sending a sequence of crafted HTTP requests to the web-based management interface of an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. Note: Cisco has assigned this security advisory a Security Impact Rating (SIR) of Critical rather than High as the score indicates. The reason is that exploitation of this vulnerability could result in an attacker elevating privileges to root.		
CVE-2025-55423	multiple ipTIME router models because the controlURL value used to pass port-forwarding information to an upper router is passed to system() without proper validation or sanitization - command injection in the upnp_relay() function	A command injection vulnerability exists in the upnp_relay() function in multiple ipTIME router models because the controlURL value used to pass port-forwarding information to an upper router is passed to system() without proper validation or sanitization, allowing OS command injection.	Patched by core rule	Y
CVE-2026-22869	Eigent is a multi-agent Workforce	Eigent is a multi-agent Workforce. A critical security vulnerability in the CI workflow (.github/workflows/ci.yml) allows arbitrary code execution from fork pull requests with repository write permissions. The vulnerable workflow uses pull_request_target trigger combined with checkout of untrusted PR code. An attacker can exploit this to steal credentials, post comments, push code, or create releases.	Patched by core rule	Y
CVE-2026-22200	Enhancesoft osTicket - arbitrary file read in the ticket PDF export functionality	Enhancesoft osTicket versions 1.18.x prior to 1.18.3 and 1.17.x prior to 1.17.7 contain an arbitrary file read vulnerability in the ticket PDF export	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality. A remote attacker can submit a ticket containing crafted rich-text HTML that includes PHP filter expressions which are insufficiently sanitized before being processed by the mPDF PDF generator during export. When the attacker exports the ticket to PDF, the generated PDF can embed the contents of attacker-selected files from the server filesystem as bitmap images, allowing disclosure of sensitive local files in the context of the osTicket application user. This issue is exploitable in default configurations where guests may create tickets and access ticket status, or where self-registration is enabled.		
CVE-2020-36875	AccessAlly WordPress plugin - unauthenticated arbitrary PHP code execution in the Login Widget	AccessAlly WordPress plugin versions prior to 3.3.2 contain an unauthenticated arbitrary PHP code execution vulnerability in the Login Widget. The plugin processes the login_error parameter as PHP code, allowing an attacker to supply and execute arbitrary PHP in the context of the WordPress web server process, resulting in remote code execution.	Patched by core rule	Y
CVE-2026-22244	OpenMetadata is a unified metadata platform	OpenMetadata is a unified metadata platform. Versions prior to 1.11.4 are vulnerable to remote code execution via Server-Side Template Injection (SSTI) in FreeMarker email templates. An attacker must have administrative privileges to exploit the vulnerability. Version 1.11.4 contains a patch.	Patched by core rule	Y
CVE-2025-55204	muffon is a cross-platform music streaming client for desktop	muffon is a cross-platform music streaming client for desktop. Versions prior to 2.3.0 have a one-click Remote Code Execution (RCE) vulnerability in. An attacker can exploit this issue by embedding a specially crafted `muffon://` link on any website they control. When a victim visits the site or clicks the link, the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		browser triggers Muffonâ€™s custom URL handler, causing the application to launch and process the URL. This leads to RCE on the victim's machine without further interaction. Version 2.3.0 patches the issue.		
CVE-2025-15421	A vulnerability was detected in Yonyou KSOA 9	A vulnerability was detected in Yonyou KSOA 9.0. This vulnerability affects unknown code of the file /worksheet/agent_worksadd.jsp of the component HTTP GET Parameter Handler. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15394	A vulnerability was detected in iCMS up to 8	A vulnerability was detected in iCMS up to 8.0.0. Affected is the function Save of the file app/config/ConfigAdmincp.php of the component POST Parameter Handler. The manipulation of the argument config results in code injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15393	A security vulnerability has been detected in Kohana KodiCMS up to 13	A security vulnerability has been detected in Kohana KodiCMS up to 13.82.135. This impacts the function Save of the file cms/modules/kodicms/classes/kodicms/model/file.php of the component Layout API Endpoint. The manipulation of the argument content leads to code injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-15257	A security flaw has been discovered in Edimax BR-6208AC 1	A security flaw has been discovered in Edimax BR-6208AC 1.02/1.03. Affected by this vulnerability is the function formRoute of the file /gogorm/formRoute of the component Web-based Configuration Interface. The manipulation of the argument strIp/strMask/strGateway results in command injection. The attack can be executed remotely. The exploit has been released to the public and may be exploited. Edimax confirms this issue: "The product mentioned, EDIMAX BR-6208AC V2, has reached its End of Life (EOL) status. It is no longer supported or maintained by Edimax, and it is no longer available for purchase in the market. Consequently, there will be no further firmware updates or patches for this device. We recommend users upgrade to newer models for better security." This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2025-15148	A flaw has been found in CmsEasy up to 7	A flaw has been found in CmsEasy up to 7.7.7. Affected is the function savetemp_action in the library /lib/admin/template_admin.php of the component Backend Template Management Page. Executing manipulation of the argument content/tempdata can lead to code injection. The attack may be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-54322	Xspeeder SXZOS through 2025-12-26 allows root remote code execution via base64-encoded Python code in the chkid parameter to vLogin	Xspeeder SXZOS through 2025-12-26 allows root remote code execution via base64-encoded Python code in the chkid parameter to vLogin.py. The title and oIP parameters are also used.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-0806	WordPress WP-ClanWars - SQLi via the 'orderby' parameter	The WP-ClanWars plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.0.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2026-24624	saeros1984 Neoforum (neoforum) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in saeros1984 Neoforum neoforum allows Blind SQL Injection.This issue affects Neoforum: from n/a through <= 1.0.	Patched by core rule	Y
CVE-2026-24572	Nelio Software Nelio Content (nelio-content) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nelio Software Nelio Content nelio-content allows Blind SQL Injection.This issue affects Nelio Content: from n/a through <= 4.1.0.	Patched by core rule	Y
CVE-2026-24367	shinetheme Traveler (traveler) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in shinetheme Traveler traveler allows Blind SQL Injection.This issue affects Traveler: from n/a through < 3.2.8.	Patched by core rule	Y
CVE-2026-22470	FireStorm Plugins FireStorm Professional Real Estate (fs-real-estate-plugin) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FireStorm Plugins FireStorm Professional Real Estate fs-real-estate-plugin allows Blind SQL Injection.This issue affects FireStorm Professional Real Estate: from n/a through <= 2.7.11.	Patched by core rule	Y
CVE-2025-69180	themepassion Ultra Portfolio (ultra-portfolio) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in themepassion Ultra Portfolio	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ultra-portfolio allows Blind SQL Injection.This issue affects Ultra Portfolio: from n/a through <= 6.7.		
CVE-2025-69045	FooEvents FooEvents for WooCommerce (fooevents) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FooEvents FooEvents for WooCommerce fooevents allows SQL Injection.This issue affects FooEvents for WooCommerce: from n/a through <= 1.20.4.	Patched by core rule	Y
CVE-2025-68999	HappyMonster Happy Addons for Elementor (happy-elementor-addons) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in HappyMonster Happy Addons for Elementor happy-elementor-addons allows Blind SQL Injection.This issue affects Happy Addons for Elementor: from n/a through <= 3.20.4.	Patched by core rule	Y
CVE-2025-68881	Saad Iqbal AppExperts (appexperts) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Saad Iqbal AppExperts appexperts allows SQL Injection.This issue affects AppExperts: from n/a through <= 1.4.5.	Patched by core rule	Y
CVE-2025-68857	ichurakov Paid Downloads (paid-downloads) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ichurakov Paid Downloads paid-downloads allows Blind SQL Injection.This issue affects Paid Downloads: from n/a through <= 3.15.	Patched by core rule	Y
CVE-2025-68034	CleverReachÂ® CleverReachÂ® WP (cleverreach-wp) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in CleverReachÂ® CleverReachÂ® WP cleverreach-wp allows SQL Injection.This issue affects CleverReachÂ® WP: from n/a through <= 1.5.22.	Patched by core rule	Y
CVE-2025-68017	Antideo Antideo Email Validator (antideo-email-validator) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Antideo Antideo Email Validator antideo-email-validator allows Blind SQL Injection.This issue affects Antideo Email Validator: from n/a through <= 1.0.10.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-67945	MailerLite MailerLite - WooCommerce integration (woo-mailerlite) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MailerLite MailerLite â€“ WooCommerce integration woo-mailerlite allows SQL Injection.This issue affects MailerLite â€“ WooCommerce integration: from n/a through <= 3.1.2.	Patched by core rule	Y
CVE-2025-49055	kamleshyadav WP Lead Capturing Pages (wp-lead-capture) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav WP Lead Capturing Pages wp-lead-capture allows Blind SQL Injection.This issue affects WP Lead Capturing Pages: from n/a through <= 2.5.	Patched by core rule	Y
CVE-2025-49050	kamleshyadav WP Lead Capturing Pages (wp-lead-capture) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in kamleshyadav WP Lead Capturing Pages wp-lead-capture allows Blind SQL Injection.This issue affects WP Lead Capturing Pages: from n/a through <= 2.5.	Patched by core rule	Y
CVE-2025-49049	ZoomIt DZS Video Gallery (dzs-videogallery) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ZoomIt DZS Video Gallery dzs-videogallery allows SQL Injection.This issue affects DZS Video Gallery: from n/a through <= 12.37.	Patched by core rule	Y
CVE-2021-47872	SEO Panel - blind SQL injection in the archive	SEO Panel versions prior to 4.9.0 contain a blind SQL injection vulnerability in the archive.php page that allows authenticated attackers to manipulate database queries through the 'order_col' parameter. Attackers can use sqlmap to exploit the vulnerability and extract database information by injecting malicious SQL code into the order column parameter.	Patched by core rule	Y
CVE-2021-47848	Blitar Tourism 1	Blitar Tourism 1.0 contains an authentication bypass vulnerability that allows attackers to bypass login by injecting SQL code through the username parameter. Attackers can manipulate the login request by sending a crafted username with SQL injection techniques to gain	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unauthorized administrative access.		
CVE-2021-47846	Digital Crime Report Management System 1	Digital Crime Report Management System 1.0 contains a critical SQL injection vulnerability affecting multiple login pages that allows unauthenticated attackers to bypass authentication. Attackers can exploit the vulnerability by sending crafted SQL injection payloads in email and password parameters across police, incharge, user, and HQ login endpoints.	Patched by core rule	Y
CVE-2026-22850	Koko Analytics is an open-source analytics plugin for WordPress	Koko Analytics is an open-source analytics plugin for WordPress. Versions prior to 2.1.3 are vulnerable to arbitrary SQL execution through unescaped analytics export/import and permissive admin SQL import. Unauthenticated visitors can submit arbitrary path (`pa`) and referrer (`r`) values to the public tracking endpoint in src/Resources/functions/collect.php, which stores those strings verbatim in the analytics tables. The admin export logic in src/Admin/Data_Export.php writes these stored values directly into SQL INSERT statements without escaping. A crafted path such as "),('999','x');DROP TABLE wp_users;-- breaks out of the value list. When an administrator later imports that export file, the import handler in src/Admin/Data_Import.php reads the uploaded SQL with file_get_contents, performs only a superficial header check, splits on semicolons, and executes each statement via $wpdb->query with no validation of table names or statement types. Additionally, any authenticated user with manage_koko_analytics can upload an arbitrary .sql file and have it executed in the same permissive way. Combined, attacker-controlled input flows from the tracking endpoint into exported SQL and through the import execution sink, or	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		directly via malicious uploads, enabling arbitrary SQL execution. In a worst-case scenario, attackers can achieve arbitrary SQL execution on the WordPress database, allowing deletion of core tables (e.g., wp_users), insertion of backdoor administrator accounts, or other destructive/privilege-escalating actions. Version 2.1.3 patches the issue.		
CVE-2025-12984	WordPress Advanced Ads - Ad Manager & AdSense - SQLi via the 'order' parameter	The Advanced Ads â€“ Ad Manager & AdSense plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter in all versions up to, and including, 2.0.15 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2026-23723	WeGIA is a web manager for charitable institutions	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, an authenticated SQL Injection vulnerability was identified in the Atendido_ocorrenciaControle endpoint via the id_memorando parameter. This flaw allows for full database exfiltration, exposure of sensitive PII, and potential arbitrary file reads in misconfigured environments. This vulnerability is fixed in 3.6.2.	Patched by core rule	Y
CVE-2021-47811	Grocery Crud - SQL injection in the order_by parameter	Grocery Crud 1.6.4 contains a SQL injection vulnerability in the order_by parameter that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through the order_by[] parameter in POST requests to the ajax_list endpoint to potentially extract or modify database information.	Patched by core rule	Y
CVE-2021-47801	Vianeos OctoPUS - time-based blind SQL injection in the 'login_user' parameter	Vianeos OctoPUS 5 contains a time-based blind SQL injection vulnerability in the 'login_user' parameter	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		during authentication requests. Attackers can exploit this vulnerability by crafting malicious POST requests with specially constructed SQL payloads that trigger database sleep functions to extract information.		
CVE-2021-47782	Odine Solutions GateKeeper - SQL injection in the trafficCycle API endpoint	Odine Solutions GateKeeper 1.0 contains a SQL injection vulnerability in the trafficCycle API endpoint that allows remote attackers to inject malicious database queries. Attackers can exploit the vulnerability by sending crafted payloads to the /rass/api/v1/trafficCycle/ endpoint to manipulate PostgreSQL database queries and potentially extract sensitive information.	Patched by core rule	Y
CVE-2025-70893	the adminprofile - time-based blind SQLi in PHPGurukul Cyber Cafe Management System v1.0	A time-based blind SQL Injection vulnerability exists in PHPGurukul Cyber Cafe Management System v1.0 within the adminprofile.php endpoint. The application fails to properly sanitize user-supplied input provided via the adminname parameter, allowing authenticated attackers to inject arbitrary SQL expressions.	Patched by core rule	Y
CVE-2025-70892	Phpgurukul Cyber Cafe Management System - SQLi in the user management module	Phpgurukul Cyber Cafe Management System v1.0 contains a SQL Injection vulnerability in the user management module. The application fails to properly validate user-supplied input in the username parameter of the add-users.php endpoint.	Patched by core rule	Y
CVE-2021-47777	Build Smart ERP - unauthenticated SQL injection in the 'eidValue' parameter	Build Smart ERP 21.0817 contains an unauthenticated SQL injection vulnerability in the 'eidValue' parameter of the login validation endpoint. Attackers can inject stacked SQL queries using payloads like ';WAITFOR DELAY '0:0:3'-- to manipulate database queries and potentially extract or modify database information.	Patched by core rule	Y
CVE-2021-47766	Kmaleon - authenticated SQL injection in the 'tipocomb' parameter	Kmaleon 1.1.0.205 contains an authenticated SQL injection vulnerability in the 'tipocomb' parameter of kmaleonW.php that allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to manipulate database queries. Attackers can exploit this vulnerability using boolean-based, error-based, and time-based blind SQL injection techniques to potentially extract or manipulate database information.		
CVE-2021-47763	Aimeos - SQL injection in the json api 'sort' parameter	Aimeos 2021.10 LTS contains a SQL injection vulnerability in the json api 'sort' parameter that allows attackers to inject malicious database queries. Attackers can manipulate the sort parameter to reveal table and column names by sending crafted GET requests to the jsonapi/review endpoint.	Patched by core rule	Y
CVE-2025-67082	An SQL injection vulnerability in InvoicePlane through 1	An SQL injection vulnerability in InvoicePlane through 1.6.3 has been identified in "maxQuantity" and "minQuantity" parameters when generating a report. An authenticated attacker can exploit this issue via error-based SQL injection, allowing for the extraction of arbitrary data from the database. The vulnerability arises from insufficient sanitizing of single quotes.	Patched by core rule	Y
CVE-2025-12166	WordPress Appointment Booking Calendar - Simply Schedule Appointments Booking Plugin - blind SQLi via the `order` and `append_where_sql` parameters	The Appointment Booking Calendar â€" Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to blind SQL Injection via the `order` and `append_where_sql` parameters in all versions up to, and including, 1.6.9.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2026-23492	Pimcore is an Open Source Data & Experience Management Platform	Pimcore is an Open Source Data & Experience Management Platform. Prior to 12.3.1 and 11.5.14, an incomplete SQL injection patch in the Admin Search Find API allows an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		authenticated attacker to perform blind SQL injection. Although CVE-2023-30848 attempted to mitigate SQL injection by removing SQL comments (--) and catching syntax errors, the fix is insufficient. Attackers can still inject SQL payloads that do not rely on comments and infer database information via blind techniques. This vulnerability affects the admin interface and can lead to database information disclosure. This vulnerability is fixed in 12.3.1 and 11.5.14.		
CVE-2025-14770	WordPress Shipping Rate By Cities - SQLi via the 'city' parameter	The Shipping Rate By Cities plugin for WordPress is vulnerable to SQL Injection via the 'city' parameter in all versions up to, and including, 2.0.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2026-0678	WordPress Flat Shipping Rate by City for WooCommerce - time-based SQLi via the 'cities' parameter	The Flat Shipping Rate by City for WooCommerce plugin for WordPress is vulnerable to time-based SQL Injection via the 'cities' parameter in all versions up to, and including, 1.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2023-54340	WorkOrder CMS 0	WorkOrder CMS 0.1.0 contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login by manipulating username and password parameters. Attackers can inject malicious SQL queries using techniques like OR	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		'1'='1' and stacked queries to access database information or execute administrative commands.		
CVE-2023-54333	Social-Share-Buttons - critical SQL injection in the project_id parameter	Social-Share-Buttons 2.2.3 contains a critical SQL injection vulnerability in the project_id parameter that allows attackers to manipulate database queries. Attackers can exploit this vulnerability by sending crafted POST requests with malicious SQL payloads to retrieve and potentially steal entire database contents.	Patched by core rule	Y
CVE-2022-50895	Aero CMS - SQL injection in the author parameter	Aero CMS 0.0.1 contains a SQL injection vulnerability in the author parameter that allows attackers to manipulate database queries. Attackers can exploit boolean-based, error-based, time-based, and UNION query techniques to extract sensitive database information and potentially compromise the system.	Patched by core rule	Y
CVE-2022-50894	VIAVIWEB Wallpaper Admin 1	VIAVIWEB Wallpaper Admin 1.0 contains an SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the img_id parameter. Attackers can send GET requests to edit_gallery_image.php with malicious img_id values to extract database information.	Patched by core rule	Y
CVE-2022-50892	VIAVIWEB Wallpaper Admin 1	VIAVIWEB Wallpaper Admin 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating login credentials. Attackers can exploit the login page by injecting 'admin' or 1=1-- - payload to gain unauthorized access to the administrative interface.	Patched by core rule	Y
CVE-2022-50805	Senayan Library Management System - SQL injection in the 'class' parameter	Senayan Library Management System 9.0.0 contains a SQL injection vulnerability in the 'class' parameter that allows attackers to inject malicious SQL queries. Attackers can exploit the vulnerability by submitting crafted payloads to manipulate database	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		queries and potentially extract sensitive information.		
CVE-2025-69991	phpgurukul News Portal Project V4	phpgurukul News Portal Project V4.1 is vulnerable to SQL Injection in check_availablity.php.	Patched by core rule	Y
CVE-2025-67146	Multiple SQL Injection vulnerabilities exist in AbhishekMali21 GYM-MANAGEMENT-SYSTEM 1	Multiple SQL Injection vulnerabilities exist in AbhishekMali21 GYM-MANAGEMENT-SYSTEM 1.0 via the 'name' parameter in (1) member_search.php, (2) trainer_search.php, and (3) gym_search.php, and via the 'id' parameter in (4) payment_search.php. An unauthenticated remote attacker can exploit these issues to inject malicious SQL commands, leading to unauthorized data extraction, authentication bypass, or modification of database contents.	Patched by core rule	Y
CVE-2025-51567	A SQL Injection was found in the /exam/user/profile	A SQL Injection was found in the /exam/user/profile.php page of kashipara Online Exam System V1.0, which allows remote attackers to execute arbitrary SQL command to get unauthorized database access via the rname, rcollage, rnumber, rgender and rpassword parameters in a POST HTTP request.	Patched by core rule	Y
CVE-2026-0852	A security flaw has been discovered in code-projects Online Music Site 1	A security flaw has been discovered in code-projects Online Music Site 1.0. The impacted element is an unknown function of the file /Administrator/PHP/AdminUpdateUser.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-0851	A vulnerability was identified in code-projects Online Music Site 1	A vulnerability was identified in code-projects Online Music Site 1.0. The affected element is an unknown function of the file /Administrator/PHP/AdminAddUser.php. The manipulation of the argument txtusername leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-0850	A vulnerability was determined in code-projects Intern Membership Management System 1	A vulnerability was determined in code-projects Intern Membership Management System 1.0. Impacted is an unknown function of the file /admin/delete_activity.php. Executing a manipulation of the argument activity_id can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-22687	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to version 0.2.5, after WeKnora enables the Agent service, it allows users to call the database query tool. Due to insufficient backend validation, an attacker can use promptâ€‘based bypass techniques to evade query restrictions and obtain sensitive information from the target server and database. This issue has been patched in version 0.2.5.	Patched by core rule	Y
CVE-2025-15496	A vulnerability was determined in guchengwuyue yshopmall up to 1	A vulnerability was determined in guchengwuyue yshopmall up to 1.9.1. Affected is the function getPage of the file /api/jobs. This manipulation of the argument sort causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15494	A vulnerability has been found in RainyGao DocSys up to 2	A vulnerability has been found in RainyGao DocSys up to 2.02.37. This affects an unknown function of the file com/DocSystem/mapping/UserMapper.xml. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15493	A flaw has been found in	A flaw has been found in	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	RainyGao DocSys up to 2	RainyGao DocSys up to 2.02.36. The impacted element is an unknown function of the file src/com/DocSystem/mapping/ReposAuthMapper.xml. Executing a manipulation of the argument searchWord can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	rule	
CVE-2026-0803	A vulnerability was found in PHPGurukul Online Course Registration System up to 3	A vulnerability was found in PHPGurukul Online Course Registration System up to 3.1. This affects an unknown part of the file /enroll.php. The manipulation of the argument studentregno/Pincode/session/department/level/course/sem results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-15492	A vulnerability was detected in RainyGao DocSys up to 2	A vulnerability was detected in RainyGao DocSys up to 2.02.36. The affected element is an unknown function of the file src/com/DocSystem/mapping/GroupMemberMapper.xml. Performing a manipulation of the argument searchWord results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-0733	A vulnerability was determined in PHPGurukul Online Course Registration System up to 3	A vulnerability was determined in PHPGurukul Online Course Registration System up to 3.1. This impacts an unknown function of the file /onlinecourse/admin/manage-students.php. This manipulation of the argument id/cid causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-0729	A vulnerability was detected in code-projects Intern Membership Management System 1	A vulnerability was detected in code-projects Intern Membership Management System 1.0. Impacted is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown function of the file /intern/admin/add_activity.php. Performing a manipulation of the argument Title results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.		
CVE-2026-0728	A security vulnerability has been detected in code-projects Intern Membership Management System 1	A security vulnerability has been detected in code-projects Intern Membership Management System 1.0. This issue affects some unknown processing of the file /intern/admin/delete_admin.php. Such manipulation of the argument admin_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-61548	SQL Injection is present on the hfInventoryDistFormID parameter in the /PSP/appNET/Store/CartV12	SQL Injection is present on the hfInventoryDistFormID parameter in the /PSP/appNET/Store/CartV12.aspx/GetUnitPrice endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34. Unsanitized user input is incorporated directly into SQL queries without proper parameterization or escaping. This vulnerability allows remote attackers to execute arbitrary SQL commands	Patched by core rule	Y
CVE-2025-61246	indieka900 online-shopping-system-php 1	indieka900 online-shopping-system-php 1.0 is vulnerable to SQL Injection in master/review_action.php via the proId parameter.	Patched by core rule	Y
CVE-2026-21892	Parsl is a Python parallel scripting library	Parsl is a Python parallel scripting library. A SQL Injection vulnerability exists in the parsl-visualize component of versions prior to 2026.01.05. The application constructs SQL queries using unsafe string formatting (Python % operator) with user-supplied input (workflow_id) directly from URL routes. This allows an unauthenticated attacker with access to the visualization dashboard to inject arbitrary SQL commands, potentially leading to data exfiltration or denial of service against the monitoring database.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Version 2026.01.05 fixes the issue.		
CVE-2026-22242	CoreShop is a Pimcore enhanced eCommerce solution	CoreShop is a Pimcore enhanced eCommerce solution. Prior to version 4.1.8, a blind SQL injection vulnerability exists in the application that allows an authenticated administrator-level user to extract database contents using boolean-based or time-based techniques. The database account used by the application is read-only and non-DBA, limiting impact to confidential data disclosure only. No data modification or service disruption is possible. This issue has been patched in version 4.1.8.	Patched by core rule	Y
CVE-2025-67928	themesuite Automotive Listings (automotive) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in themesuite Automotive Listings automotive allows Blind SQL Injection.This issue affects Automotive Listings: from n/a through <= 18.6.	Patched by core rule	Y
CVE-2025-67921	VanKarWai Lobo (lobo) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VanKarWai Lobo lobo allows Blind SQL Injection.This issue affects Lobo: from n/a through < 2.8.6.	Patched by core rule	Y
CVE-2025-23993	RiceTheme Felan Framework (felan-framework) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RiceTheme Felan Framework felan-framework allows SQL Injection.This issue affects Felan Framework: from n/a through <= 1.1.3.	Patched by core rule	Y
CVE-2025-22728	AmentoTech Workreap (theme's plugin) (workreap) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AmentoTech Workreap (theme's plugin) workreap allows SQL Injection.This issue affects Workreap (theme's plugin): from n/a through <= 3.3.6.	Patched by core rule	Y
CVE-2025-22713	vanquish WooCommerce Orders & Customers Exporter (woocommerce-orders-ei) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in vanquish WooCommerce Orders & Customers	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Exporter woocommerce-orders-ei allows SQL Injection.This issue affects WooCommerce Orders & Customers Exporter: from n/a through <= 5.4.		
CVE-2026-0701	A vulnerability was identified in code-projects Intern Membership Management System 1	A vulnerability was identified in code-projects Intern Membership Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /intern/admin/add_admin.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-0700	A vulnerability was determined in code-projects Intern Membership Management System 1	A vulnerability was determined in code-projects Intern Membership Management System 1.0. Affected is an unknown function of the file /intern/admin/check_admin.php. Executing a manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-0699	A vulnerability was found in code-projects Intern Membership Management System 1	A vulnerability was found in code-projects Intern Membership Management System 1.0. This impacts an unknown function of the file /intern/admin/edit_activity.php. Performing a manipulation of the argument activity_id results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-0698	A vulnerability has been found in code-projects Intern Membership Management System 1	A vulnerability has been found in code-projects Intern Membership Management System 1.0. This affects an unknown function of the file /intern/admin/edit_students.php. Such manipulation of the argument admin_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-0697	A flaw has been found in code-projects Intern	A flaw has been found in code-projects Intern	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Membership Management System 1	Membership Management System 1.0. The impacted element is an unknown function of the file /intern/admin/edit_admin.php. This manipulation of the argument admin_id causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.		
CVE-2026-21875	ClipBucket v5 is an open source video sharing platform	ClipBucket v5 is an open source video sharing platform. Versions 5.5.2-#187 and below allow an attacker to perform Blind SQL Injection through the add comment section within a channel. When adding a comment within a channel, there is a POST request to the /actions/ajax.php endpoint. The obj_id parameter within the POST request to /actions/ajax.php is then used within the user_exists function of the upload/includes/classes/user.class. php file as the $id parameter. It is then used within the count function of the upload/includes/classes/db.class. php file. The $id parameter is concatenated into the query without validation or sanitization, and a user-supplied input like 1' or 1=1-- - can be used to trigger the injection. This issue does not have a fix at the time of publication.	Patched by core rule	Y
CVE-2025-32303	Mojoomla (WPCHURCH) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mojoomla WPCHURCH allows Blind SQL Injection.This issue affects WPCHURCH: from n/a through 2.7.0.	Patched by core rule	Y
CVE-2025-14719	The Relevanssi WordPress plugin before 4	The Relevanssi WordPress plugin before 4.26.0, Relevanssi Premium WordPress plugin before 2.29.0 do not sanitize and escape a parameter before using it in a SQL statement, allowing contributor and above roles to perform SQL injection attacks	Patched by core rule	Y
CVE-2025-69351	Shahjahan Jewel Ninja Tables (ninja-tables) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Shahjahan Jewel Ninja Tables ninja-tables allows Blind SQL Injection.This issue affects Ninja Tables: from n/a through <= 5.2.4.		
CVE-2025-9318	WordPress Quiz and Survey Master (QSM) - Easy Quiz and Survey Maker - time-based SQLi via the 'is_linking' parameter	The Quiz and Survey Master (QSM) â€“ Easy Quiz and Survey Maker plugin for WordPress is vulnerable to time-based SQL Injection via the â€˜is_linkingâ€™ parameter in all versions up to, and including, 10.3.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-14153	WordPress Page Expire Popup/Redirection for WordPress - time-based SQLi via the 'id' shortcode attribute	The Page Expire Popup/Redirection for WordPress plugin for WordPress is vulnerable to time-based SQL Injection via the 'id' shortcode attribute in all versions up to, and including, 1.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2025-13652	WordPress CBX Bookmark & Favorite - generic SQLi via the 'orderby' parameter	The CBX Bookmark & Favorite plugin for WordPress is vulnerable to generic SQL Injection via the â€˜orderbyâ€™ parameter in all versions up to, and including, 2.0.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the database.		
CVE-2025-13409	WordPress Form Vibes - Database Manager for Forms - SQLi via the 'params' parameter	The Form Vibes â€“ Database Manager for Forms plugin for WordPress is vulnerable to SQL Injection via the 'params' parameter in all versions up to, and including, 1.4.13 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	Patched by core rule	Y
CVE-2026-0607	A flaw has been found in code-projects Online Music Site 1	A flaw has been found in code-projects Online Music Site 1.0. This affects an unknown part of the file /Administrator/PHP/AdminViewSongs.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-0606	A vulnerability was detected in code-projects Online Music Site 1	A vulnerability was detected in code-projects Online Music Site 1.0. Affected by this issue is some unknown functionality of the file /FrontEnd/Albums.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-0605	A security vulnerability has been detected in code-projects Online Music Site 1	A security vulnerability has been detected in code-projects Online Music Site 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. Such manipulation of the argument username/password leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2025-39484	Waituk (Entrada) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Waituk Entrada allows SQL Injection.This issue affects Entrada: from n/a through 5.7.7.		
CVE-2026-0597	A flaw has been found in Campcodes Supplier Management System 1	A flaw has been found in Campcodes Supplier Management System 1.0. Affected by this issue is some unknown functionality of the file /retailer/edit_profile.php. This manipulation of the argument txtRetailerAddress causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-0592	A security flaw has been discovered in code-projects Online Product Reservation System 1	A security flaw has been discovered in code-projects Online Product Reservation System 1.0. This affects an unknown function of the file /handgunner-administrator/register_code.php of the component User Registration Handler. Performing a manipulation of the argument fname/lname/address/city/province/country/zip/tel_no/email/username results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-0591	A vulnerability was identified in code-projects Online Product Reservation System 1	A vulnerability was identified in code-projects Online Product Reservation System 1.0. The impacted element is an unknown function of the file /app/checkout/update.php of the component Cart Update Handler. Such manipulation of the argument id/qty leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-0590	A vulnerability was determined in code-projects Online Product Reservation System 1	A vulnerability was determined in code-projects Online Product Reservation System 1.0. The affected element is an unknown function of the file /app/checkout/delete.php of the component POST Parameter Handler. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been publicly disclosed and may be utilized.		
CVE-2025-68865	Infility Infility (Global) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Infility Infility Global allows SQL Injection.This issue affects Infility Global: from n/a through 2.14.48.	Patched by core rule	Y
CVE-2025-31044	AA-Team Premium SEO (Pack) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Premium SEO Pack allows SQL Injection.This issue affects Premium SEO Pack: from n/a through 3.3.2.	Patched by core rule	Y
CVE-2025-30633	AA-Team Amazon Native Shopping (Recommendations) - SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Amazon Native Shopping Recommendations allows SQL Injection.This issue affects Amazon Native Shopping Recommendations: from n/a through 1.3.	Patched by core rule	Y
CVE-2026-0585	A security vulnerability has been detected in code-projects Online Product Reservation System 1	A security vulnerability has been detected in code-projects Online Product Reservation System 1.0. Impacted is an unknown function of the file /order_view.php of the component GET Parameter Handler. Such manipulation of the argument transaction_id leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-0584	A weakness has been identified in code-projects Online Product Reservation System 1	A weakness has been identified in code-projects Online Product Reservation System 1.0. This issue affects some unknown processing of the file app/products/left_cart.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-0583	A security flaw has been discovered in code-projects Online Product	A security flaw has been discovered in code-projects Online Product Reservation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Reservation System 1	System 1.0. This vulnerability affects unknown code of the file app/user/login.php of the component User Login. The manipulation of the argument emailadd results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.		
CVE-2026-0582	A vulnerability was identified in itsourcecode Society Management System 1	A vulnerability was identified in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/edit_activity_query.php. The manipulation of the argument Title leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-0581	A vulnerability was determined in Tenda AC1206 15	A vulnerability was determined in Tenda AC1206 15.03.06.23. Affected by this issue is the function formBehaviorManager of the file /goform/BehaviorManager of the component httpd. Executing a manipulation of the argument modulename/option/data/switch can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-14124	The Team WordPress plugin before 5	The Team WordPress plugin before 5.0.11 does not properly sanitize and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	Patched by core rule	Y
CVE-2025-15447	A vulnerability has been found in Seeyon Zhiyuan OA Web Application System up to 20251223	A vulnerability has been found in Seeyon Zhiyuan OA Web Application System up to 20251223. This affects an unknown function of the file /assetsGroupReport/assetsService.j%73p. The manipulation of the argument unitCode leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is still unclear if this vulnerability genuinely exists. Seeyon	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		filed a report that this issue does not affect their product but might affect a product of another vendor.		
CVE-2025-15446	A flaw has been found in Seeyon Zhiyuan OA Web Application System up to 20251223	A flaw has been found in Seeyon Zhiyuan OA Web Application System up to 20251223. The impacted element is an unknown function of the file /assetsGroupReport/fixedAssetsList.j%73p. Executing a manipulation of the argument unitCode can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used. The real existence of this vulnerability is still doubted at the moment. Seeyon filed a report that this issue does not affect their product but might affect a product of another vendor.	Patched by core rule	Y
CVE-2026-0579	A vulnerability was found in code-projects Online Product Reservation System 1	A vulnerability was found in code-projects Online Product Reservation System 1.0. This affects an unknown part of the file /handgunner-administrator/edit.php of the component POST Parameter Handler. The manipulation of the argument prod_id/name/price/model/serial results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-0578	A vulnerability has been found in code-projects Online Product Reservation System 1	A vulnerability has been found in code-projects Online Product Reservation System 1.0. Affected by this issue is some unknown functionality of the file /handgunner-administrator/delete.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-15443	A vulnerability was identified in CRMEB up to 5	A vulnerability was identified in CRMEB up to 5.6.1. This issue affects some unknown processing of the file /adminapi/product/product_export. Such manipulation of the argument cate_id leads to sql injection. The attack may be launched	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-15442	A vulnerability was determined in CRMEB up to 5	A vulnerability was determined in CRMEB up to 5.6.1. This vulnerability affects unknown code of the file /adminapi/export/product_list. This manipulation of the argument cate_id causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-0576	A vulnerability was detected in code-projects Online Product Reservation System 1	A vulnerability was detected in code-projects Online Product Reservation System 1.0. Affected is an unknown function of the file /handgunner-administrator/prod.php of the component Parameter Handler. Performing manipulation of the argument cat/price/name/model/serial results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-0575	A security vulnerability has been detected in code-projects Online Product Reservation System 1	A security vulnerability has been detected in code-projects Online Product Reservation System 1.0. This impacts an unknown function of the file /handgunner-administrator/adminlogin.php of the component Administrator Login. Such manipulation of the argument emailadd/pass leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-0570	A vulnerability was found in code-projects Online Music Site 1	A vulnerability was found in code-projects Online Music Site 1.0. This impacts an unknown function of the file /Frontend/Feedback.php. Performing manipulation of the argument fname results in sql injection. The attack can be initiated remotely. The exploit has been made	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		public and could be used.		
CVE-2026-0569	A vulnerability has been found in code-projects Online Music Site 1	A vulnerability has been found in code-projects Online Music Site 1.0. This affects an unknown function of the file /Frontend/AlbumByCategory.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-0568	A flaw has been found in code-projects Online Music Site 1	A flaw has been found in code-projects Online Music Site 1.0. The impacted element is an unknown function of the file /Frontend/ViewSongs.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-0567	A vulnerability was detected in code-projects Content Management System 1	A vulnerability was detected in code-projects Content Management System 1.0. The affected element is an unknown function of the file /pages.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-65125	SQL injection in gosaliajainam/online-movie-booking 5	SQL injection in gosaliajainam/online-movie-booking 5.5 in movie_details.php allows attackers to gain sensitive information.	Patched by core rule	Y
CVE-2026-0565	A weakness has been identified in code-projects Content Management System 1	A weakness has been identified in code-projects Content Management System 1.0. This issue affects some unknown processing of the file /admin/delete.php. Executing manipulation of the argument del can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-0546	A vulnerability was determined in code-projects Content Management System 1	A vulnerability was determined in code-projects Content Management System 1.0. This impacts an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		search.php. This manipulation of the argument Value causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.		
CVE-2025-15436	A vulnerability has been found in Yonyou KSOA 9	A vulnerability has been found in Yonyou KSOA 9.0. Affected by this issue is some unknown functionality of the file /worksheet/work_edit.jsp. Such manipulation of the argument Report leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15435	A flaw has been found in Yonyou KSOA 9	A flaw has been found in Yonyou KSOA 9.0. Affected by this vulnerability is an unknown functionality of the file /worksheet/work_update.jsp. This manipulation of the argument Report causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15434	A vulnerability was detected in Yonyou KSOA 9	A vulnerability was detected in Yonyou KSOA 9.0. Affected is an unknown function of the file /kp/PrintZPYG.jsp. The manipulation of the argument zpjhid results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15427	A security flaw has been discovered in Seeyon Zhiyuan OA Web Application System up to 20251222	A security flaw has been discovered in Seeyon Zhiyuan OA Web Application System up to 20251222. This impacts an unknown function of the file /carManager/carUseDetailList.j%73p. The manipulation of the argument CAR_BRAND_NO results in sql injection. The attack may be performed from remote.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been released to the public and may be used for attacks. The existence of this vulnerability is still disputed at present. Seeyon filed a report that this issue does not affect their product but might affect a product of another vendor.		
CVE-2025-15425	A vulnerability was determined in Yonyou KSOA 9	A vulnerability was determined in Yonyou KSOA 9.0. The impacted element is an unknown function of the file /worksheet/del_user.jsp of the component HTTP GET Parameter Handler. Executing manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15424	A vulnerability was found in Yonyou KSOA 9	A vulnerability was found in Yonyou KSOA 9.0. The affected element is an unknown function of the file /worksheet/agent_worksdel.jsp of the component HTTP GET Parameter Handler. Performing manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15420	A security vulnerability has been detected in Yonyou KSOA 9	A security vulnerability has been detected in Yonyou KSOA 9.0. This affects an unknown part of the file /worksheet/agent_work_report.jsp. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15410	A vulnerability was identified in code-projects Online Guitar Store 1	A vulnerability was identified in code-projects Online Guitar Store 1.0. Affected by this issue is some unknown functionality of the file /login.php. The manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument L_email leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.		
CVE-2025-15409	A vulnerability was determined in code-projects Online Guitar Store 1	A vulnerability was determined in code-projects Online Guitar Store 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/Delete_product.php. Executing manipulation of the argument del_pro can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-15408	A vulnerability was found in code-projects Online Guitar Store 1	A vulnerability was found in code-projects Online Guitar Store 1.0. Affected is an unknown function of the file /admin/Create_product.php. Performing manipulation of the argument dre_title results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-15407	A vulnerability has been found in code-projects Online Guitar Store 1	A vulnerability has been found in code-projects Online Guitar Store 1.0. This impacts an unknown function of the file /admin/Create_category.php. Such manipulation of the argument dre_Ctitle leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-0544	A security flaw has been discovered in itsourcecode School Management System 1	A security flaw has been discovered in itsourcecode School Management System 1.0. This affects an unknown part of the file /student/index.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2025-30628	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Amazon Affiliates Addon for...	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AA-Team Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer) allows SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Injection.This issue affects Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer): from n/a through 1.2.		
CVE-2025-28949	Codedraft Mediabay - WordPress Media Library (Folders) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Codedraft Mediabay - WordPress Media Library Folders allows Blind SQL Injection.This issue affects Mediabay - WordPress Media Library Folders: from n/a through 1.4.	Patched by core rule	Y
CVE-2022-50694	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x - SQL injection in the 'username' POST parameter	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains an SQL injection vulnerability in the 'username' POST parameter of index.php that allows attackers to manipulate database queries. Attackers can inject arbitrary SQL code through the username parameter to bypass authentication and potentially access unauthorized database information.	Patched by core rule	Y
CVE-2025-15354	A flaw has been found in itsourcecode Society Management System 1	A flaw has been found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/add_admin.php. Executing manipulation of the argument Username can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-15353	A vulnerability was detected in itsourcecode Society Management System 1	A vulnerability was detected in itsourcecode Society Management System 1.0. Impacted is the function edit_admin_query of the file /admin/edit_admin_query.php. Performing manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-15263	A weakness has been identified in BiggiDroid Simple PHP CMS 1	A weakness has been identified in BiggiDroid Simple PHP CMS 1.0. Affected is an unknown function of the file /admin/login.php of the component Admin Login. Executing manipulation of the argument Username can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.		
CVE-2025-59129	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Appointify allows Blind SQL Injection	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Appointify allows Blind SQL Injection.This issue affects Appointify: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-68990	xenioushk BWL Pro Voting Manager (bwl-pro-voting-manager) - Blind SQLi	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in xenioushk BWL Pro Voting Manager bwl-pro-voting-manager allows Blind SQL Injection.This issue affects BWL Pro Voting Manager: from n/a through <= 1.4.9.	Patched by core rule	Y
CVE-2025-15243	A flaw has been found in code-projects Simple Stock System 1	A flaw has been found in code-projects Simple Stock System 1.0. This affects an unknown function of the file /market/login.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-15212	A vulnerability was detected in code-projects Refugee Food Management System 1	A vulnerability was detected in code-projects Refugee Food Management System 1.0. This issue affects some unknown processing of the file /home/regfood.php. Performing manipulation of the argument a results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-15211	A flaw has been found in code-projects Refugee Food Management System 1	A flaw has been found in code-projects Refugee Food Management System 1.0. Impacted is an unknown function of the file /home/refugee.php. Executing manipulation of the argument refNo/Fname/Lname/sex/age/contact/nationality_nid can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-15210	A security vulnerability	A security vulnerability has	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	has been detected in code-projects Refugee Food Management System 1	been detected in code-projects Refugee Food Management System 1.0. This vulnerability affects unknown code of the file /home/editrefugee.php. Such manipulation of the argument a/b/c/sex/d/e/nationality_nid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	rule	
CVE-2025-15209	A weakness has been identified in code-projects Refugee Food Management System 1	A weakness has been identified in code-projects Refugee Food Management System 1.0. This affects an unknown part of the file /home/editfood.php. This manipulation of the argument a/b/c/d causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-15208	A security flaw has been discovered in code-projects Refugee Food Management System 1	A security flaw has been discovered in code-projects Refugee Food Management System 1.0. Affected by this issue is some unknown functionality of the file /home/editrefugee.php. The manipulation of the argument rfid results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-15207	A vulnerability has been found in Campcodes Supplier Management System 1	A vulnerability has been found in Campcodes Supplier Management System 1.0. Affected is an unknown function of the file /admin/view_products.php. The manipulation of the argument chkId[] leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-15206	A flaw has been found in Campcodes Supplier Management System 1	A flaw has been found in Campcodes Supplier Management System 1.0. This impacts an unknown function of the file /admin/add_area.php. Executing manipulation of the argument txtAreaCode can lead to sql injection. The attack may be performed from remote. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been published and may be used.		
CVE-2025-15205	A vulnerability was identified in code-projects Student File Management System 1	A vulnerability was identified in code-projects Student File Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /download.php. The manipulation of the argument istore_id leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-15198	A weakness has been identified in code-projects College Notes Uploading System 1	A weakness has been identified in code-projects College Notes Uploading System 1.0. This issue affects some unknown processing of the file /login.php. Executing manipulation of the argument User can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be exploited.	Patched by core rule	Y
CVE-2025-15196	A vulnerability was identified in code-projects Assessment Management 1	A vulnerability was identified in code-projects Assessment Management 1.0. This affects an unknown part of the file login.php. Such manipulation of the argument userid leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2025-15195	A vulnerability was determined in code-projects Assessment Management 1	A vulnerability was determined in code-projects Assessment Management 1.0. Affected by this issue is some unknown functionality of the file /admin/add-module.php. This manipulation of the argument linked[] causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-15186	A vulnerability has been found in code-projects Refugee Food Management System 1	A vulnerability has been found in code-projects Refugee Food Management System 1.0. Affected by this issue is some unknown functionality of the file /home/addusers.php. Such manipulation of the argument a leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be used.		
CVE-2025-15185	A flaw has been found in code-projects Refugee Food Management System 1	A flaw has been found in code-projects Refugee Food Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /home/refugeesreport.php. This manipulation of the argument a causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2025-15181	A security flaw has been discovered in code-projects Refugee Food Management System 1	A security flaw has been discovered in code-projects Refugee Food Management System 1.0. The impacted element is an unknown function of the file /home/pagenateRefugeesList.php. Performing manipulation of the argument rfid results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.	Patched by core rule	Y
CVE-2025-13417	The Plugin Organizer WordPress plugin before 10	The Plugin Organizer WordPress plugin before 10.2.4 does not sanitize and escape a parameter before using it in a SQL statement, allowing subscribers to perform SQL injection attacks.	Patched by core rule	Y
CVE-2025-15169	A weakness has been identified in BiggiDroid Simple PHP CMS 1	A weakness has been identified in BiggiDroid Simple PHP CMS 1.0. Affected by this issue is some unknown functionality of the file /admin/editsite.php. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15168	A vulnerability was identified in itsourcecode Student Management System 1	A vulnerability was identified in itsourcecode Student Management System 1.0. Affected is an unknown function of the file /statistical.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit is publicly available and might be used.		
CVE-2025-15167	A vulnerability was determined in itsourcecode Online Cake Ordering System 1	A vulnerability was determined in itsourcecode Online Cake Ordering System 1.0. This impacts an unknown function of the file /detailtransac.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-15166	A vulnerability was found in itsourcecode Online Cake Ordering System 1	A vulnerability was found in itsourcecode Online Cake Ordering System 1.0. This affects an unknown function of the file /updatesupplier.php?action =edit. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2025-15165	A vulnerability has been found in itsourcecode Online Cake Ordering System 1	A vulnerability has been found in itsourcecode Online Cake Ordering System 1.0. The impacted element is an unknown function of the file /updatecustomer.php?actio n=edit. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2025-15143	A security flaw has been discovered in EyouCMS up to 1	A security flaw has been discovered in EyouCMS up to 1.7.6. The affected element is an unknown function of the file /application/admin/logic/Fil emanagerLogic.php of the component Backend Template Management. The manipulation of the argument content results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be exploited. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-66947	SQL injection vulnerability in krishanmuraiji SMS v	SQL injection vulnerability in krishanmuraiji SMS v.1.0, within the /studentms/admin/edit-class-detail.php via the editid GET parameter. An attacker can trigger	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		controlled delays using SQL SLEEP() to infer database contents. Successful exploitation may lead to full database compromise, especially within an administrative module.		

Server-Side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-47899	YetiShare File Hosting Script 5	YetiShare File Hosting Script 5.1.0 contains a server-side request forgery vulnerability that allows attackers to read local system files through the remote file upload feature. Attackers can exploit the url parameter in the url_upload_handler endpoint to access sensitive files like /etc/passwd by using file:/// protocol.	Patched by core rule	Y
CVE-2025-15104	Nu Html Checker (validator	Nu Html Checker (validator.nu) contains a restriction bypass that allows remote attackers to make the server perform arbitrary HTTP/HTTPS requests to internal resources, including localhost services. While the validator implements hostname-based protections to block direct access to localhost and 127.0.0.1, these controls can be bypassed using DNS rebinding techniques or domains that resolve to loopback addresses.This issue affects The Nu Html Checker (vnu): latest (commit 23f090a11bab8d0d4e698f1ffc197a4fe226a9cd).	Patched by core rule	Y
CVE-2026-23768	lucy-xss-filter before commit 7c1de6d allows an attacker to induce server-side HEAD requests to arbitrary URLs when the ObjectSecurityLis...	lucy-xss-filter before commit 7c1de6d allows an attacker to induce server-side HEAD requests to arbitrary URLs when the ObjectSecurityListener or EmbedSecurityListener option is enabled and embed or object tags are used with a src attribute missing a file extension.	Patched by core rule	Y
CVE-2021-47776	Umbraco CMS v8	Umbraco CMS v8.14.1 contains a server-side request forgery vulnerability that allows attackers to manipulate baseUrl parameters in multiple dashboard and help controller endpoints. Attackers can craft malicious requests to the GetContextHelpForPage, GetRemoteDashboardContent, and GetRemoteDashboardCss endpoints to trigger unauthorized server-side requests to external hosts.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-21885	Miniflux 2 is an open source feed reader	Miniflux 2 is an open source feed reader. Prior to version 2.2.16, Miniflux's media proxy endpoint (`GET /proxy/{encodedDigest}/{encodedURL}`) can be abused to perform Server-Side Request Forgery (SSRF). An authenticated user can cause Miniflux to generate a signed proxy URL for attacker-chosen media URLs embedded in feed entry content, including internal addresses (e.g., localhost, private RFC1918 ranges, or link-local metadata endpoints). Requesting the resulting `/proxy/...` URL makes Miniflux fetch and return the internal response. Version 2.2.16 fixes the issue.	Patched by core rule	Y
CVE-2019-25290	Smartliving SmartLAN/G/SI <=6.x - unauthenticated server-side request forgery in the GetImage functionality through the 'host' parameter	Smartliving SmartLAN/G/SI <=6.x contains an unauthenticated server-side request forgery vulnerability in the GetImage functionality through the 'host' parameter. Attackers can exploit the onvif.cgi endpoint by specifying external domains to bypass firewalls and perform network enumeration through arbitrary HTTP requests.	Patched by core rule	Y
CVE-2025-69222	LibreChat is a ChatGPT clone with additional features	LibreChat is a ChatGPT clone with additional features. Version 0.8.1-rc2 is prone to a server-side request forgery (SSRF) vulnerability due to missing restrictions of the Actions feature in the default configuration. LibreChat enables users to configure agents with predefined instructions and actions that can interact with remote services via OpenAPI specifications, supporting various HTTP methods, parameters, and authentication methods including custom headers. By default, there are no restrictions on accessible services, which means agents can also access internal components like the RAG API included in the default Docker Compose setup. This issue is fixed in version 0.8.1-rc2.	Patched by core rule	Y
CVE-2025-68437	Craft is a platform for	Craft is a platform for	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	creating digital experiences	creating digital experiences. In versions 5.0.0-RC1 through 5.8.20 and 4.0.0-RC1 through 4.16.16, the Craft CMS GraphQL `save_<VolumeName>_Asset` mutation is vulnerable to Server-Side Request Forgery (SSRF). This vulnerability arises because the `_file` input, specifically its `url` parameter, allows the server to fetch content from arbitrary remote locations without proper validation. Attackers can exploit this by providing internal IP addresses or cloud metadata endpoints as the `url`, forcing the server to make requests to these restricted services. The fetched content is then saved as an asset, which can subsequently be accessed and exfiltrated, leading to potential data exposure and infrastructure compromise. This exploitation requires specific GraphQL permissions for asset management within the targeted volume. Users should update to the patched 5.8.21 and 4.16.17 releases to mitigate the issue.	rule	
CVE-2026-21433	Emlog is an open source website building system	Emlog is an open source website building system. Versions up to and including 2.5.19 are vulnerable to server-side Out-of-Band (OOB) requests / SSRF via uploaded SVG files. An attacker can upload a crafted SVG to http[:]//emblog/admin/media[.]php which contains external resource references. When the server processes/renders the SVG (thumbnailing, preview, or sanitization), it issues an HTTP request to the attacker-controlled host. Impact: server-side SSRF/OOB leading to internal network probing and potential metadata/credential exposure. As of time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2026-21428	cpp-httplib is a C++11 single-file header-only	cpp-httplib is a C++11 single-file header-only cross	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross platform HTTP/HTTPS library	platform HTTP/HTTPS library. Prior to version 0.30.0, the ``write_headers`` function does not check for CR & LF characters in user supplied headers, allowing untrusted header value to escape header lines. This vulnerability allows attackers to add extra headers, modify request body unexpectedly & trigger an SSRF attack. When combined with a server that supports http1.1 pipelining (springboot, python twisted etc), this can be used for server side request forgery (SSRF). Version 0.30.0 fixes this issue.		
CVE-2025-34469	Cowrie - server-side request forgery (SSRF) in the emulated shell implementation of wget and curl	Cowrie versions prior to 2.9.0 contain a server-side request forgery (SSRF) vulnerability in the emulated shell implementation of wget and curl. In the default emulated shell configuration, these command emulations perform real outbound HTTP requests to attacker-supplied destinations. Because no outbound request rate limiting was enforced, unauthenticated remote attackers could repeatedly invoke these commands to generate unbounded HTTP traffic toward arbitrary third-party targets, allowing the Cowrie honeypot to be abused as a denial-of-service amplification node and masking the attackerâ€™s true source address behind the honeypotâ€™s IP.	Patched by core rule	Y
CVE-2025-15373	A security vulnerability has been detected in EyouCMS up to 1	A security vulnerability has been detected in EyouCMS up to 1.7.7. Impacted is the function saveRemote of the file application/function.php. Such manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor is "[a]cknowledging the existence of the vulnerability, we have completed the fix and will release a new version, v1.7.8".	Patched by core rule	Y
CVE-2025-69206	Hemmelig is a messing	Hemmelig is a messing app	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	app with with client-side encryption and self-destructing messages	with with client-side encryption and self-destructing messages. Prior to version 7.3.3, a Server-Side Request Forgery (SSRF) filter bypass vulnerability exists in the webhook URL validation of the Secret Requests feature. The application attempts to block internal/private IP addresses but can be bypassed using DNS rebinding or open redirect services. This allows an authenticated user to make the server initiate HTTP requests to internal network resources. Version 7.3.3 contains a patch for the issue.	rule	
CVE-2025-15098	A vulnerability was determined in YunaiV yudao-cloud up to 2025	A vulnerability was determined in YunaiV yudao-cloud up to 2025.11. This affects the function BpmHttpCallbackTrigger/BpmSyncHttpRequestTrigger of the component Business Process Management. Executing manipulation of the argument url/header/body can lead to server-side request forgery. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-70457	the gallery/upload - Remote Code Execution (RCE) in Sourcecodester Modern Image Gallery App v1.0	A Remote Code Execution (RCE) vulnerability exists in Sourcecodester Modern Image Gallery App v1.0 within the gallery/upload.php component. The application fails to properly validate uploaded file contents. Additionally, the application preserves the user-supplied file extension during the save process. This allows an unauthenticated attacker to upload arbitrary PHP code by spoofing the MIME type as an image, leading to full system compromise.	Patched by core rule	Y
CVE-2021-47904	PhreeBooks - authenticated file upload in the Image Manager	PhreeBooks 5.2.3 contains an authenticated file upload vulnerability in the Image Manager that allows remote code execution. Attackers can upload a malicious PHP web shell by exploiting unrestricted file type uploads to gain command execution on the server.	Patched by core rule	Y
CVE-2021-47888	Textpattern versions prior to 4	Textpattern versions prior to 4.8.3 contain an authenticated remote code execution vulnerability that allows logged-in users to upload malicious PHP files. Attackers can upload a PHP file with a shell command execution payload and execute arbitrary commands by accessing the uploaded file through a specific URL parameter.	Patched by core rule	Y
CVE-2026-24010	Horilla is a free and open source Human Resource Management System (HRMS)	Horilla is a free and open source Human Resource Management System (HRMS). A critical File Upload vulnerability in versions prior to 1.5.0, with Social Engineering, allows authenticated users to deploy phishing attacks. By uploading a malicious HTML file disguised as a profile picture, an attacker can create a convincing login page replica that steals user credentials. When a victim visits the uploaded file URL, they see an authentic-looking "Session Expired" message prompting them to re-authenticate. All entered credentials are captured and sent to the attacker's server,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		enabling Account Takeover. Version 1.5.0 patches the issue.		
CVE-2026-1107	A weakness has been identified in EyouCMS up to 1	A weakness has been identified in EyouCMS up to 1.7.1/5.0. Impacted is the function check_userinfo of the file Diyajax.php of the component Member Avatar Handler. Executing a manipulation of the argument viewfile can lead to unrestricted upload. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2021-47783	Phpwcms 1	Phpwcms 1.9.30 contains a file upload vulnerability that allows authenticated attackers to upload malicious SVG files with embedded JavaScript. Attackers can upload crafted SVG payloads through the multiple file upload feature to potentially execute cross-site scripting attacks on the platform.	Patched by core rule	Y
CVE-2011-10041	Uploadify WordPress plugin - arbitrary file upload in process_upload	Uploadify WordPress plugin versions up to and including 1.0 contain an arbitrary file upload vulnerability in process_upload.php due to missing file type validation. An unauthenticated remote attacker can upload arbitrary files to the affected WordPress site, which may allow remote code execution by uploading executable content to a web-accessible location.	Patched by core rule	Y
CVE-2021-47758	Chikitsa Patient Management System 2	Chikitsa Patient Management System 2.0.2 contains an authenticated remote code execution vulnerability that allows attackers to upload malicious PHP plugins through the module upload functionality. Authenticated attackers can generate and upload a ZIP plugin with a PHP backdoor that enables arbitrary command execution on the server through a weaponized PHP script.	Patched by core rule	Y
CVE-2021-47757	Chikitsa Patient Management System -	Chikitsa Patient Management System 2.0.2	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	authenticated remote code execution in the backup restoration functionality	contains an authenticated remote code execution vulnerability in the backup restoration functionality. Authenticated attackers can upload a modified backup zip file with a malicious PHP shell to execute arbitrary system commands on the server.		
CVE-2021-47753	phpKF CMS 3	phpKF CMS 3.00 Beta y6 contains an unauthenticated file upload vulnerability that allows remote attackers to execute arbitrary code by bypassing file extension checks. Attackers can upload a PHP file disguised as a PNG, rename it, and execute system commands through a crafted web shell parameter.	Patched by core rule	Y
CVE-2022-50936	WBCE CMS version 1	WBCE CMS version 1.5.2 contains an authenticated remote code execution vulnerability that allows attackers to upload malicious droplets through the admin panel. Authenticated attackers can exploit the droplet upload functionality in the admin tools to create and execute arbitrary PHP code by crafting a specially designed zip file payload.	Patched by core rule	Y
CVE-2022-50912	ImpressCMS 1	ImpressCMS 1.4.4 contains a file upload vulnerability with weak extension sanitization that allows attackers to upload potentially malicious files. Attackers can bypass file upload restrictions by using alternative file extensions .php2.php6.php7.phps.pht to execute arbitrary PHP code on the server.	Patched by core rule	Y
CVE-2022-50907	e107 CMS version 3	e107 CMS version 3.2.1 contains a file upload vulnerability that allows authenticated administrative users to bypass upload restrictions and execute PHP files. Attackers can upload malicious PHP files to parent directories by manipulating the upload URL parameter, enabling remote code execution through the Media Manager import feature.	Patched by core rule	Y
CVE-2022-50893	VIAVIWEB Wallpaper Admin - unauthenticated remote code execution in the image upload	VIAVIWEB Wallpaper Admin 1.0 contains an unauthenticated remote code execution vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	functionality	in the image upload functionality. Attackers can upload a malicious PHP file through the add_gallery_image.php endpoint to execute arbitrary code on the server.		
CVE-2025-69992	phpgurukul News Portal Project V4	phpgurukul News Portal Project V4.1 has File Upload Vulnerability via upload.php, which enables the upload of files of any format to the server without identity authentication.	Patched by core rule	Y
CVE-2026-22799	Emlog is an open source website building system	Emlog is an open source website building system. emlog v2.6.1 and earlier exposes a REST API endpoint (/index.php?rest-api=upload) for media file uploads. The endpoint fails to implement proper validation of file types, extensions, and content, allowing authenticated attackers (with a valid API key or admin session cookie) to upload arbitrary files (including malicious PHP scripts) to the server. An attacker can obtain the API key either by gaining administrator access to enable the REST API setting, or via information disclosure vulnerabilities in the application. Once uploaded, the malicious PHP file can be executed to gain remote code execution (RCE) on the target server, leading to full server compromise.	Patched by core rule	Y
CVE-2024-27480	givanz VvvebJs 1	givanz VvvebJs 1.7.2 is vulnerable to Insecure File Upload.	Patched by core rule	Y
CVE-2024-25182	givanz VvvebJs 1	givanz VvvebJs 1.7.2 suffers from a File Upload vulnerability via save.php.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-20613	The ArchiveReader	The ArchiveReader.extractContents() function used by cctl image load and container image load performs no pathname validation before extracting an archive member. This means that a carelessly or maliciously constructed archive can extract a file into any user-writable location on the system using relative pathnames. This issue is addressed in container 0.8.0 and containerization 0.21.0.	Patched by core rule	Y
CVE-2023-7335	EduSoho - arbitrary file read in the classroom-course-statistics export functionality	EduSoho versions prior to 22.4.7 contain an arbitrary file read vulnerability in the classroom-course-statistics export functionality. A remote, unauthenticated attacker can supply crafted path traversal sequences in the fileNames[] parameter to read arbitrary files from the server filesystem, including application configuration files such as config/parameters.yml that may contain secrets and database credentials. Exploitation evidence was observed by the Shadowserver Foundation on 2026-01-19 (UTC).	Patched by core rule	Y
CVE-2021-47795	GeoVision GeoWebServer 5	GeoVision GeoWebServer 5.3.3 contains multiple vulnerabilities including local file inclusion, cross-site scripting, and remote code execution through improper input sanitization. Attackers can exploit the WebStrings.srf endpoint by manipulating path traversal and injection parameters to access system files and execute malicious scripts.	Patched by core rule	Y
CVE-2017-20212	FLIR Thermal Camera F/FC/PT/D firmware version 8	FLIR Thermal Camera F/FC/PT/D firmware version 8.0.0.64 contains an information disclosure vulnerability that allows unauthenticated attackers to read arbitrary files through unverified input parameters. Attackers can exploit the /var/www/data/controllers/api/xml.php readFile() function to access local system files without authentication.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-67366	@sylphxltd/filesystem-mcp - critical path traversal in its "read_content" tool	@sylphxltd/filesystem-mcp v0.5.8 is an MCP server that provides file content reading functionality. Version 0.5.8 of filesystem-mcp contains a critical path traversal vulnerability in its "read_content" tool. This vulnerability arises from improper symlink handling in the path validation mechanism: the resolvePath function checks path validity before resolving symlinks, while fs.readFile resolves symlinks automatically during file access. This allows attackers to bypass directory restrictions by leveraging symlinks within the allowed directory that point to external files, enabling unauthorized access to files outside the intended operational scope.	Patched by core rule	Y
CVE-2022-50796	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x - unauthenticated remote code execution in the firmware upload functionality with path traversal flaw	SOUND4 IMPACT/FIRST/PULSE/Eco <=2.x contains an unauthenticated remote code execution vulnerability in the firmware upload functionality with path traversal flaw. Attackers can exploit the upload.cgi script to write malicious files to the system with www-data permissions, enabling unauthorized access and code execution.	Patched by core rule	Y
CVE-2025-57403	Cola Dnslog v1	Cola Dnslog v1.3.2 is vulnerable to Directory Traversal. When a DNS query for a TXT record is processed, the application concatenates the requested URL (or a portion of it) directly with a base path using os.path.join. This bypass allows directory traversal or absolute path injection, leading to the potential exposure of sensitive information.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-36932	SeaCMS - stored cross-site scripting in the checkuser parameter	SeaCMS 11.1 contains a stored cross-site scripting vulnerability in the checkuser parameter of the admin settings page. Attackers can inject malicious JavaScript payloads that will execute in users' browsers when the page is loaded.	Patched by core rule	Y
CVE-2020-36931	Click2Magic 1	Click2Magic 1.1.5 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts in the chat name input. Attackers can craft a malicious payload in the chat name to capture administrator cookies when the admin processes user requests.	Patched by core rule	Y
CVE-2026-0862	WordPress Save as PDF Plugin by PDFCrowd - Reflected XSS via the 'options' parameter	The Save as PDF Plugin by PDFCrowd plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the â€˜optionsâ€™ parameter in all versions up to, and including, 4.5.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. NOTE: Successful exploitation of this vulnerability requires that the PDFCrowd API key is blank (also known as "demo mode", which is the default configuration when the plugin is installed) or known.	Patched by core rule	Y
CVE-2026-1302	WordPress Meta-box GalleryMeta - Stored XSS via admin settings	The Meta-box GalleryMeta plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		where unfiltered_html has been disabled.		
CVE-2026-1300	WordPress Responsive Header - Stored XSS via multiple plugin settings parameters	The Responsive Header plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple plugin settings parameters in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2026-1266	WordPress Postalicious - Stored XSS via admin settings	The Postalicious plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2026-1191	WordPress JavaScript Notifier - Stored XSS via plugin settings	The JavaScript Notifier plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin settings in all versions up to, and including, 1.2.8. This is due to insufficient input sanitization and output escaping on user-supplied attributes in the `wp_footer` action. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-1189	WordPress LeadBI Plugin for WordPress - Stored XSS via the 'form_id' parameter	The LeadBI Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_id' parameter	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the 'leadbi_form' shortcode in all versions up to, and including, 1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-1127	WordPress Timeline Event History - Reflected XSS via the `id` parameter	The Timeline Event History plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `id` parameter in all versions up to, and including, 3.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2026-1098	WordPress CM CSS Columns - Stored XSS via the 'tag' shortcode attribute	The CM CSS Columns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' shortcode attribute in all versions up to, and including, 1.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-0800	WordPress User Submitted Posts - Enable Users to Submit Posts from the Front End - Stored XSS via the custom fields	The User Submitted Posts â€“ Enable Users to Submit Posts from the Front End plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the custom fields in all versions up to, and including, 20251210 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-1099	WordPress Administrative	The Administrative Shortcodes plugin for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Shortcodes - Stored XSS via the 'login' and 'logout' shortcode attributes	WordPress is vulnerable to Stored Cross-Site Scripting via the 'login' and 'logout' shortcode attributes in all versions up to, and including, 0.3.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-1097	WordPress ThemeRuby Multi Authors - Assign Multiple Writers to Posts - Stored XSS via the 'before' and 'after' shortcode attributes	The ThemeRuby Multi Authors â€“ Assign Multiple Writers to Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'before' and 'after' shortcode attributes in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-1095	WordPress Canto Testimonials - Stored XSS via the 'fx' shortcode attribute	The Canto Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fx' shortcode attribute in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-1084	WordPress Cookie consent for developers - Stored XSS via multiple settings fields	The Cookie consent for developers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple settings fields in all versions up to, and including, 1.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.		
CVE-2025-14985	WordPress Alpha Blocks - Stored XSS via the 'alpha_block_css' parameter	The Alpha Blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the â€˜alpha_block_cssâ€™ parameter in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14941	WordPress GZSEO - authorization bypass leading to Stored XSS	The GZSEO plugin for WordPress is vulnerable to authorization bypass leading to Stored Cross-Site Scripting in all versions up to, and including, 2.0.11. This is due to missing capability checks on multiple AJAX handlers combined with insufficient input sanitization and output escaping on the embed_code parameter. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary content into any post on the site that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14797	WordPress Same Category Posts - Stored XSS via the widget title placeholder functionality	The Same Category Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the widget title placeholder functionality in all versions up to, and including, 1.1.19. This is due to the use of `htmlspecialchars_decode()` on taxonomy term names before output, which decodes HTML entities that WordPress intentionally encodes for safety. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-13676	WordPress JustClick registration - Reflected XSS	The JustClick registration plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in all versions up to, and including, 0.1. This is due to insufficient input sanitization and output escaping on the `PHP_SELF` server variable. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-12836	The VK Google Job Posting Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Job Description field in vers...	The VK Google Job Posting Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Job Description field in versions up to, and including, 1.2.20 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers with author-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-70458	domain/script - DOM-based XSS (XSS) in the DomainCheckerApp class	A DOM-based Cross-Site Scripting (XSS) vulnerability exists in the DomainCheckerApp class within domain/script.js of Sourcecodester Domain Availability Checker v1.0. The vulnerability occurs because the application improperly handles user-supplied data in the createResultElement method by using the unsafe innerHTML property to render domain search results.	Patched by core rule	Y
CVE-2025-71177	LavaLite CMS - stored cross-site scripting in the package creation and search functionality	LavaLite CMS versions up to and including 10.1.0 contain a stored cross-site scripting vulnerability in the package creation and search functionality. Authenticated users can supply crafted HTML or JavaScript in the package Name or Description fields that is stored and later rendered without proper output encoding in package search results. When other users view search results that	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		include the malicious package, the injected script executes in their browsers, potentially enabling session hijacking, credential theft, and unauthorized actions in the context of the victim.		
CVE-2021-47906	BloofoxCMS - stored cross-site scripting in the articles text parameter	BloofoxCMS 0.5.2.1 contains a stored cross-site scripting vulnerability in the articles text parameter that allows authenticated attackers to inject malicious scripts. Attackers can insert malicious javascript payloads in the text field to execute scripts and potentially steal authenticated users' cookies.	Patched by core rule	Y
CVE-2021-47905	MyBB Delete Account Plugin - cross-site scripting in the account deletion reason input field	MyBB Delete Account Plugin 1.4 contains a cross-site scripting vulnerability in the account deletion reason input field. Attackers can inject malicious scripts that will execute in the admin interface when viewing delete account reasons.	Patched by core rule	Y
CVE-2021-47897	PEEL Shopping - stored cross-site scripting in the address parameter	PEEL Shopping 9.3.0 contains a stored cross-site scripting vulnerability in the address parameter of the change_params.php script. Attackers can inject malicious JavaScript payloads that execute when users interact with the address text box, potentially enabling client-side script execution.	Patched by core rule	Y
CVE-2021-47892	PEEL Shopping - stored cross-site scripting in the 'Comments / Special Instructions' parameter	PEEL Shopping 9.3.0 contains a stored cross-site scripting vulnerability in the 'Comments / Special Instructions' parameter of the purchase page. Attackers can inject malicious JavaScript payloads that will execute when the page is refreshed, potentially allowing client-side script execution.	Patched by core rule	Y
CVE-2018-25132	MyBB Trending Widget Plugin 1	MyBB Trending Widget Plugin 1.2 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through thread titles. Attackers can modify thread titles with script payloads that will execute when other users view the trending widget.	Patched by core rule	Y
CVE-2018-25116	MyBB Thread Redirect	MyBB Thread Redirect	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Plugin - cross-site scripting in the custom text input field for thread redirects	Plugin 0.2.1 contains a cross-site scripting vulnerability in the custom text input field for thread redirects. Attackers can inject malicious SVG scripts that will execute when other users view the thread, allowing arbitrary script execution.	rule	
CVE-2026-24632	jagdish1o1 Delay Redirects (delay-redirects) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jagdish1o1 Delay Redirects delay-redirects allows DOM-Based XSS.This issue affects Delay Redirects: from n/a through <= 1.0.0.	Patched by core rule	Y
CVE-2026-24630	Design Stylish Cost Calculator (stylish-cost-calculator) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Design Stylish Cost Calculator stylish-cost-calculator allows Stored XSS.This issue affects Stylish Cost Calculator: from n/a through <= 8.1.8.	Patched by core rule	Y
CVE-2026-24629	Ability, Inc Web Accessibility with Max Access (accessibility-toolbar) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ability, Inc Web Accessibility with Max Access accessibility-toolbar allows Stored XSS.This issue affects Web Accessibility with Max Access: from n/a through <= 2.1.0.	Patched by core rule	Y
CVE-2026-24626	LogicHunt Logo Slider (logo-slider-wp) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LogicHunt Logo Slider logo-slider-wp allows Stored XSS.This issue affects Logo Slider: from n/a through <= 4.9.0.	Patched by core rule	Y
CVE-2026-24623	saeros1984 Neoforum (neoforum) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in saeros1984 Neoforum neoforum allows Reflected XSS.This issue affects Neoforum: from n/a through <= 1.0.	Patched by core rule	Y
CVE-2026-24621	Vladimir Statsenko Terms descriptions (terms-descriptions) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vladimir Statsenko Terms descriptions terms-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		descriptions allows DOM-Based XSS.This issue affects Terms descriptions: from n/a through <= 3.4.9.		
CVE-2026-24620	PluginOps Landing Page Builder (page-builder-add) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginOps Landing Page Builder page-builder-add allows Stored XSS.This issue affects Landing Page Builder: from n/a through <= 1.5.3.3.	Patched by core rule	Y
CVE-2026-24617	Daniel Iser Easy Modal (easy-modal) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daniel Iser Easy Modal easy-modal allows Stored XSS.This issue affects Easy Modal: from n/a through <= 2.1.0.	Patched by core rule	Y
CVE-2026-24614	Devsbrain Flex QR Code Generator (flex-qr-code-generator) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Devsbrain Flex QR Code Generator flex-qr-code-generator allows DOM-Based XSS.This issue affects Flex QR Code Generator: from n/a through <= 1.2.8.	Patched by core rule	Y
CVE-2026-24601	PenciDesign Penci Pay Writer (penci-pay-writer) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Pay Writer penci-pay-writer allows Stored XSS.This issue affects Penci Pay Writer: from n/a through <= 1.5.	Patched by core rule	Y
CVE-2026-24600	PenciDesign Penci Review (penci-review) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Review penci-review allows Stored XSS.This issue affects Penci Review: from n/a through <= 3.5.	Patched by core rule	Y
CVE-2026-24594	livemesh Livemesh Addons for WPBakery Page Builder (addons-for-visual-composer) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in livemesh Livemesh Addons for WPBakery Page Builder addons-for-visual-composer allows Stored XSS.This issue affects Livemesh Addons for WPBakery Page Builder: from n/a through <= 3.9.4.	Patched by core rule	Y
CVE-2026-24591	yasir129 Turn Yoast SEO FAQ Block to Accordion (faq-schema-block-to-accordion) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		yasir129 Turn Yoast SEO FAQ Block to Accordion faq-schema-block-to-accordion allows Stored XSS.This issue affects Turn Yoast SEO FAQ Block to Accordion: from n/a through <= 1.0.6.		
CVE-2026-24584	Themeum Tutor LMS BunnyNet Integration (tutor-lms-bunnynet-integration) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Tutor LMS BunnyNet Integration tutor-lms-bunnynet-integration allows DOM-Based XSS.This issue affects Tutor LMS BunnyNet Integration: from n/a through <= 1.0.0.	Patched by core rule	Y
CVE-2026-24576	COP UX Flat (ux-flat) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in COP UX Flat ux-flat allows Stored XSS.This issue affects UX Flat: from n/a through <= 5.4.0.	Patched by core rule	Y
CVE-2026-24558	antoniobg ABG Rich Pins (abg-rich-pins) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in antoniobg ABG Rich Pins abg-rich-pins allows Stored XSS.This issue affects ABG Rich Pins: from n/a through <= 1.1.	Patched by core rule	Y
CVE-2026-24555	artplacer ArtPlacer Widget (artplacer-widget) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in artplacer ArtPlacer Widget artplacer-widget allows Stored XSS.This issue affects ArtPlacer Widget: from n/a through <= 2.23.1.	Patched by core rule	Y
CVE-2026-24550	Kaira Blockons (blockons) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kaira Blockons blockons allows Stored XSS.This issue affects Blockons: from n/a through <= 1.2.15.	Patched by core rule	Y
CVE-2026-24528	pixelgrade Nova Blocks (nova-blocks) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixelgrade Nova Blocks nova-blocks allows DOM-Based XSS.This issue affects Nova Blocks: from n/a through <= 2.1.9.	Patched by core rule	Y
CVE-2026-24526	Steve Truman Email Inquiry & Cart Options for WooCommerce	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	(woocommerce-email-inquiry-cart-options) - DOM-Based XSS	Scripting') vulnerability in Steve Truman Email Inquiry & Cart Options for WooCommerce woocommerce-email-inquiry-cart-options allows DOM-Based XSS.This issue affects Email Inquiry & Cart Options for WooCommerce: from n/a through <= 3.4.3.		
CVE-2026-0914	WordPress WP DSGVO Tools (GDPR) - Stored XSS via the plugin's 'lw_content_block' shortcode	The WP DSGVO Tools (GDPR) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'lw_content_block' shortcode in all versions up to, and including, 3.1.36 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14745	WordPress RSS Aggregator - RSS Import, News Feeds, Feed to Post, and Autoblogging - Stored XSS via the plugin's 'wp-rss-aggregator' shortcode	The RSS Aggregator â€“ RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wp-rss-aggregator' shortcode in all versions up to, and including, 5.0.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14069	WordPress Schema & Structured Data for WP & AMP - Stored XSS via the 'saswp_custom_schema_field' profile field	The Schema & Structured Data for WP & AMP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'saswp_custom_schema_field' profile field in all versions up to, and including, 1.54 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injected page.		
CVE-2025-15522	WordPress Uncanny Automator - Easy Automation, Integration, Webhooks & Workflow Builder Plugin - Stored XSS via the automator_discord_user_mapping shortcode	The Uncanny Automator â€“ Easy Automation, Integration, Webhooks & Workflow Builder Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the automator_discord_user_mapping shortcode in all versions up to, and including, 6.10.0.2 due to insufficient input sanitization and output escaping on the verified_message parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user with a verified Discord account accesses the injected page.	Patched by core rule	Y
CVE-2026-24389	WP Chill Gallery PhotoBlocks (photoblocks-grid-gallery) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Gallery PhotoBlocks photoblocks-grid-gallery allows DOM-Based XSS.This issue affects Gallery PhotoBlocks: from n/a through <= 1.3.2.	Patched by core rule	Y
CVE-2026-24383	bPlugins B Slider (b-slider) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bPlugins B Slider b-slider allows DOM-Based XSS.This issue affects B Slider: from n/a through <= 2.0.6.	Patched by core rule	Y
CVE-2026-24361	ThimPress LearnPress – Course Review (learnpress-course-review) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress – Course Review learnpress-course-review allows Stored XSS.This issue affects LearnPress – Course Review: from n/a through <= 4.1.9.	Patched by core rule	Y
CVE-2026-24355	favethemes Houzez Theme - Functionality (houzez-theme-functionality) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Houzez Theme - Functionality houzez-theme-functionality allows Stored XSS.This issue affects Houzez Theme - Functionality: from n/a through <= 4.2.6.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-24354	PenciDesign Penci Shortcodes & Performance (penci-shortcodes) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Penci Shortcodes & Performance penci-shortcodes allows DOM-Based XSS.This issue affects Penci Shortcodes & Performance: from n/a through <= 6.1.	Patched by core rule	Y
CVE-2026-23976	WP Chill Modula Image Gallery (modula-best-grid-gallery) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Chill Modula Image Gallery modula-best-grid-gallery allows Stored XSS.This issue affects Modula Image Gallery: from n/a through <= 2.13.4.	Patched by core rule	Y
CVE-2026-22463	Micro.company Form to Chat App (form-to-chat) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Micro.company Form to Chat App form-to-chat allows Stored XSS.This issue affects Form to Chat App: from n/a through <= 1.2.5.	Patched by core rule	Y
CVE-2026-22388	Imran Emu Owl Carousel WP (owl-carousel-wp) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imran Emu Owl Carousel WP owl-carousel-wp allows Stored XSS.This issue affects Owl Carousel WP: from n/a through <= 2.2.2.	Patched by core rule	Y
CVE-2026-22353	winkm89 teachPress (teachpress) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in winkm89 teachPress teachpress allows Stored XSS.This issue affects teachPress: from n/a through <= 9.0.12.	Patched by core rule	Y
CVE-2026-22349	linux4me2 Menu In Post (menu-in-post) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in linux4me2 Menu In Post menu-in-post allows DOM-Based XSS.This issue affects Menu In Post: from n/a through <= 1.4.1.	Patched by core rule	Y
CVE-2026-22347	subhansanjaya Carousel Horizontal Posts Content Slider (carousel-horizontal-posts-content-slider) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in subhansanjaya Carousel Horizontal Posts Content Slider carousel-horizontal-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		posts-content-slider allows DOM-Based XSS.This issue affects Carousel Horizontal Posts Content Slider: from n/a through <= 3.3.2.		
CVE-2025-69321	ThemeGoods Grand Spa (grandspa) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Spa grandspa allows Reflected XSS.This issue affects Grand Spa: from n/a through <= 3.5.5.	Patched by core rule	Y
CVE-2025-69320	ThemeGoods Grand Magazine (grandmagazine) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Magazine grandmagazine allows Reflected XSS.This issue affects Grand Magazine: from n/a through <= 3.5.7.	Patched by core rule	Y
CVE-2025-69318	Hossni Mubarak JobWP (jobwp) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hossni Mubarak JobWP jobwp allows Stored XSS.This issue affects JobWP: from n/a through <= 2.4.5.	Patched by core rule	Y
CVE-2025-69317	scriptsbundle CarSpot (carspot) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in scriptsbundle CarSpot carspot allows Reflected XSS.This issue affects CarSpot: from n/a through < 2.4.6.	Patched by core rule	Y
CVE-2025-69316	RealMag777 TableOn (posts-table-filterable) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in RealMag777 TableOn posts-table-filterable allows Reflected XSS.This issue affects TableOn: from n/a through <= 1.0.4.2.	Patched by core rule	Y
CVE-2025-69102	Boopathi Rajan WP Test Email (wp-test-email) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Boopathi Rajan WP Test Email wp-test-email allows Reflected XSS.This issue affects WP Test Email: from n/a through <= 1.1.7.	Patched by core rule	Y
CVE-2025-69098	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpWave Hide My WP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpWave Hide My WP	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	hide_my_wp allows...	hide_my_wp allows Reflected XSS.This issue affects Hide My WP: from n/a through <= 6.2.12.		
CVE-2025-69056	e-plugins Hotel Listing (hotel-listing) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Hotel Listing hotel-listing allows Reflected XSS.This issue affects Hotel Listing: from n/a through <= 1.4.0.	Patched by core rule	Y
CVE-2025-69054	highwarden Super Logos Showcase (superlogoshowcase-wp) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in highwarden Super Logos Showcase superlogoshowcase-wp allows Reflected XSS.This issue affects Super Logos Showcase: from n/a through <= 2.8.	Patched by core rule	Y
CVE-2025-69053	LambertGroup Universal Video Player (universal-video-player) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player universal-video-player allows Reflected XSS.This issue affects Universal Video Player: from n/a through <= 3.8.4.	Patched by core rule	Y
CVE-2025-69051	CridioStudio ListingPro Reviews (listingpro-reviews) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CridioStudio ListingPro Reviews listingpro-reviews allows Reflected XSS.This issue affects ListingPro Reviews: from n/a through <= 1.7.	Patched by core rule	Y
CVE-2025-69048	LambertGroup Universal Video Player (universal-video-player) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Universal Video Player universal-video-player allows Reflected XSS.This issue affects Universal Video Player: from n/a through <= 3.8.4.	Patched by core rule	Y
CVE-2025-69003	QantumThemes KenthaRadio (qt-kentharadio) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in QantumThemes KenthaRadio qt-kentharadio allows Reflected XSS.This issue affects KenthaRadio:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		from n/a through <= 2.2.0.		
CVE-2025-68906	jegtheme JNews - Video (jnews-video) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jegtheme JNews - Video jnews-video allows Reflected XSS.This issue affects JNews - Video: from n/a through <= 11.0.2.	Patched by core rule	Y
CVE-2025-68904	jegtheme JNews - Frontend Submit (jnews-frontend-submit) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jegtheme JNews - Frontend Submit jnews-frontend-submit allows Reflected XSS.This issue affects JNews - Frontend Submit: from n/a through <= 11.0.0.	Patched by core rule	Y
CVE-2025-68900	Kriesi Enfold (enfold) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kriesi Enfold enfold allows DOM-Based XSS.This issue affects Enfold: from n/a through <= 7.1.3.	Patched by core rule	Y
CVE-2025-68898	cjjparadoxmax Synergy Project Manager (synergy-project-manager) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in cjjparadoxmax Synergy Project Manager synergy-project-manager allows Stored XSS.This issue affects Synergy Project Manager: from n/a through <= 1.5.	Patched by core rule	Y
CVE-2025-68894	shoutoutglobal ShoutOut (shoutout) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in shoutoutglobal ShoutOut shoutout allows Reflected XSS.This issue affects ShoutOut: from n/a through <= 4.0.2.	Patched by core rule	Y
CVE-2025-68884	Arevico WP Simple Redirect (wp-simple-redirect) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arevico WP Simple Redirect wp-simple-redirect allows Reflected XSS.This issue affects WP Simple Redirect: from n/a through <= 1.1.	Patched by core rule	Y
CVE-2025-68883	extremeidea bidorbuy Store Integrator (bidorbuystoreintegrator) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in extremeidea bidorbuy Store Integrator bidorbuystoreintegrator	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows Reflected XSS.This issue affects bidorbuy Store Integrator: from n/a through <= 2.12.0.		
CVE-2025-68871	noCreativity Dooodl (dooodl) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in noCreativity Dooodl dooodl allows Reflected XSS.This issue affects Dooodl: from n/a through <= 2.3.0.	Patched by core rule	Y
CVE-2025-68866	woofer696 Dinatur (dinatur) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in woofer696 Dinatur dinatur allows Stored XSS.This issue affects Dinatur: from n/a through <= 1.18.	Patched by core rule	Y
CVE-2025-68864	Infility Infility Global (infility-global) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Infility Infility Global infility-global allows Stored XSS.This issue affects Infility Global: from n/a through <= 2.14.50.	Patched by core rule	Y
CVE-2025-68859	agmorpheus Syntax Highlighter Compress (syntax-highlighter-compress) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in agmorpheus Syntax Highlighter Compress syntax-highlighter-compress allows Reflected XSS.This issue affects Syntax Highlighter Compress: from n/a through <= 3.0.83.3.	Patched by core rule	Y
CVE-2025-68858	Casey Bisson wpCAS (wpcas) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Casey Bisson wpCAS wpcas allows Reflected XSS.This issue affects wpCAS: from n/a through <= 1.07.	Patched by core rule	Y
CVE-2025-68849	Frank Corso Quote Master (quote-master) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Frank Corso Quote Master quote-master allows Reflected XSS.This issue affects Quote Master: from n/a through <= 7.1.1.	Patched by core rule	Y
CVE-2025-68839	Remi Corson Easy Theme Options (easy-theme-options) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Remi Corson Easy Theme Options easy-theme-options allows Reflected XSS.This issue affects Easy Theme	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Options: from n/a through <= 1.0.		
CVE-2025-68838	expresstechsoftware MemberPress Discord Addon (expresstechsoftwares-memberpress-discord-add-on) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in expresstechsoftware MemberPress Discord Addon expresstechsoftwares-memberpress-discord-add-on allows Reflected XSS.This issue affects MemberPress Discord Addon: from n/a through <= 1.1.4.	Patched by core rule	Y
CVE-2025-68835	matiskiba Ravpage (ravpage) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matiskiba Ravpage ravpage allows Reflected XSS.This issue affects Ravpage: from n/a through <= 2.33.	Patched by core rule	Y
CVE-2025-68538	ThemeGoods Craft (craftcoffee) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Craft craftcoffee allows DOM-Based XSS.This issue affects Craft: from n/a through <= 2.3.6.	Patched by core rule	Y
CVE-2025-68520	ThemeGoods DotLife (dotlife) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods DotLife dotlife allows Reflected XSS.This issue affects DotLife: from n/a through < 4.9.5.	Patched by core rule	Y
CVE-2025-68518	ThemeGoods Hoteller (hoteller) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Hoteller hoteller allows Reflected XSS.This issue affects Hoteller: from n/a through < 6.8.9.	Patched by core rule	Y
CVE-2025-68041	codisto Omnichannel for WooCommerce (codistoconnect) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codisto Omnichannel for WooCommerce codistoconnect allows Stored XSS.This issue affects Omnichannel for WooCommerce: from n/a through <= 1.3.65.	Patched by core rule	Y
CVE-2025-68012	Dmytro Shteflyuk CodeColorer (codecolorer) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Dmytro Shteflyuk CodeColorer codecolorer allows Stored XSS.This issue affects CodeColorer: from n/a through <= 0.10.1.		
CVE-2025-68011	GLS GLS Shipping for WooCommerce (gls-shipping-for-woocommerce) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GLS GLS Shipping for WooCommerce gls-shipping-for-woocommerce allows Reflected XSS.This issue affects GLS Shipping for WooCommerce: from n/a through <= 1.4.0.	Patched by core rule	Y
CVE-2025-68010	netgsm Netgsm (netgsm) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in netgsm Netgsm netgsm allows Reflected XSS.This issue affects Netgsm: from n/a through <= 2.9.63.	Patched by core rule	Y
CVE-2025-68008	mndpsingh287 WP Mail (wp-mail) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in mndpsingh287 WP Mail wp-mail allows Reflected XSS.This issue affects WP Mail: from n/a through <= 1.3.	Patched by core rule	Y
CVE-2025-68004	Kapil Chugh My Post Order (my-posts-order) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kapil Chugh My Post Order my-posts-order allows Reflected XSS.This issue affects My Post Order: from n/a through <= 1.2.1.1.	Patched by core rule	Y
CVE-2025-67964	favethemes Homey Core (homey-core) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in favethemes Homey Core homey-core allows Reflected XSS.This issue affects Homey Core: from n/a through <= 2.4.3.	Patched by core rule	Y
CVE-2025-67960	purethemes WorkScout-Core (workscout-core) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes WorkScout-Core workscout-core allows Reflected XSS.This issue affects WorkScout-Core: from n/a through <= 1.7.06.	Patched by core rule	Y
CVE-2025-67959	purethemes WorkScout (workscout) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		purethemes WorkScout workscout allows Reflected XSS.This issue affects WorkScout: from n/a through <= 4.1.07.		
CVE-2025-67952	ThemeGoods Grand Tour (grandtour) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Tour grandtour allows Reflected XSS.This issue affects Grand Tour: from n/a through < 5.6.2.	Patched by core rule	Y
CVE-2025-67949	designingmedia Hostiko (hostiko) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designingmedia Hostiko hostiko allows Reflected XSS.This issue affects Hostiko: from n/a through < 94.3.6.	Patched by core rule	Y
CVE-2025-67947	scriptsbundle AdForest Elementor (adforest-elementor) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in scriptsbundle AdForest Elementor adforest-elementor allows Reflected XSS.This issue affects AdForest Elementor: from n/a through <= 3.0.11.	Patched by core rule	Y
CVE-2025-67943	wphocus My auctions allegro (my-auctions-allegro-free-edition) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wphocus My auctions allegro my-auctions-allegro-free-edition allows Reflected XSS.This issue affects My auctions allegro: from n/a through <= 3.6.32.	Patched by core rule	Y
CVE-2025-67923	Crocoblock JetEngine (jet-engine) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine jet-engine allows Reflected XSS.This issue affects JetEngine: from n/a through <= 3.7.7.	Patched by core rule	Y
CVE-2025-67620	CleverSoft Anon (anon2x) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CleverSoft Anon anon2x allows Reflected XSS.This issue affects Anon: from n/a through <= 2.2.10.	Patched by core rule	Y
CVE-2025-67614	foreverpinetree TheNa (thena) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		foreverpinetree TheNa thena allows Reflected XSS.This issue affects TheNa: from n/a through <= 1.5.5.		
CVE-2025-63026	ThemeGoods Grand Restaurant Theme Elements for Elementor (grandrestaurant-elementor) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Restaurant Theme Elements for Elementor grandrestaurant-elementor allows Stored XSS.This issue affects Grand Restaurant Theme Elements for Elementor: from n/a through <= 2.1.1.	Patched by core rule	Y
CVE-2025-62077	SEOSEON EUROPE S.L Affiliate Link Tracker (affiliate-link-tracker) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SEOSEON EUROPE S.L Affiliate Link Tracker affiliate-link-tracker allows Stored XSS.This issue affects Affiliate Link Tracker: from n/a through <= 0.2.	Patched by core rule	Y
CVE-2025-53240	adamlabs WordPress Photo Gallery (photo-gallery-portfolio) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in adamlabs WordPress Photo Gallery photo-gallery-portfolio allows Reflected XSS.This issue affects WordPress Photo Gallery: from n/a through <= 1.1.0.	Patched by core rule	Y
CVE-2025-52762	flexostudio flexo-posts-manager (flexo-posts-manager) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in flexostudio flexo-posts-manager flexo-posts-manager allows Reflected XSS.This issue affects flexo-posts-manager: from n/a through <= 1.0001.	Patched by core rule	Y
CVE-2025-52746	ayecode Restaurante (restaurante) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ayecode Restaurante restaurante allows Reflected XSS.This issue affects Restaurante: from n/a through <= 3.0.7.	Patched by core rule	Y
CVE-2025-50006	Jthemes xSmart (xsmart) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jthemes xSmart xsmart allows Reflected XSS.This issue affects xSmart: from n/a through <= 1.2.9.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-50005	tagDiv tagDiv Composer (td-composer) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in tagDiv tagDiv Composer td-composer allows DOM-Based XSS.This issue affects tagDiv Composer: from n/a through <= 5.4.2.	Patched by core rule	Y
CVE-2025-49336	pondol Pondol BBS (pondol-bbs) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pondol Pondol BBS pondol-bbs allows Stored XSS.This issue affects Pondol BBS: from n/a through <= 1.1.8.4.	Patched by core rule	Y
CVE-2025-49249	ApusTheme Drone (drone) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ApusTheme Drone drone allows Reflected XSS.This issue affects Drone: from n/a through <= 1.40.	Patched by core rule	Y
CVE-2025-49066	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Accordion Slider PRO a...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Accordion Slider PRO accordion_slider_pro allows Reflected XSS.This issue affects Accordion Slider PRO: from n/a through <= 1.2.	Patched by core rule	Y
CVE-2025-49046	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup xPromoter top_bar_prom...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup xPromoter top_bar_promoter allows Reflected XSS.This issue affects xPromoter: from n/a through <= 1.3.4.	Patched by core rule	Y
CVE-2025-49045	highwarden Super Interactive Maps (super-interactive-maps) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in highwarden Super Interactive Maps super-interactive-maps allows Reflected XSS.This issue affects Super Interactive Maps: from n/a through <= 2.3.	Patched by core rule	Y
CVE-2025-49043	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Magic Responsive Slide...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Magic Responsive Slider and Carousel WordPress magic_carousel allows Reflected XSS.This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects Magic Responsive Slider and Carousel WordPress: from n/a through <= 1.6.		
CVE-2025-48094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Magic Slider magic_sli...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Magic Slider magic_slider allows Reflected XSS.This issue affects Magic Slider: from n/a through <= 2.2.	Patched by core rule	Y
CVE-2025-47666	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Image&Video FullScreen...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Image&Video FullScreen Background lbg_fullscreen_fullwidth_slider allows Reflected XSS.This issue affects Image&Video FullScreen Background: from n/a through <= 1.6.7.	Patched by core rule	Y
CVE-2025-47500	Benjamin Intal Stackable (stackable-ultimate-gutenberg-blocks) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Benjamin Intal Stackable stackable-ultimate-gutenberg-blocks allows Stored XSS.This issue affects Stackable: from n/a through <= 3.19.5.	Patched by core rule	Y
CVE-2025-32123	LambertGroup HTML5 Video Player with Playlist & Multiple Skins (lbg-vp2-html5-rightside) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup HTML5 Video Player with Playlist & Multiple Skins lbg-vp2-html5-rightside allows Reflected XSS.This issue affects HTML5 Video Player with Playlist & Multiple Skins: from n/a through <= 5.3.5.	Patched by core rule	Y
CVE-2025-27005	LambertGroup HTML5 Video Player (lbg-vp2-html5-bottom) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup HTML5 Video Player lbg-vp2-html5-bottom allows Reflected XSS.This issue affects HTML5 Video Player: from n/a through <= 5.3.5.	Patched by core rule	Y
CVE-2025-65098	Typebot is an open-source chatbot builder	Typebot is an open-source chatbot builder. In versions prior to 3.13.2, client-side script execution in Typebot allows stealing all stored credentials from any user. When a victim previews a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		malicious typebot by clicking "Run", JavaScript executes in their browser and exfiltrates their OpenAI keys, Google Sheets tokens, and SMTP passwords. The `/api/trpc/credentials.getCredentials` endpoint returns plaintext API keys without verifying credential ownership. Version 3.13.2 fixes the issue.		
CVE-2026-24037	Horilla is a free and open source Human Resource Management System (HRMS)	Horilla is a free and open source Human Resource Management System (HRMS). In version 1.4.0, the has_xss() function attempts to block XSS by matching input against a set of regex patterns. However, the regexes are incomplete and context-agnostic, making them easy to bypass. Attackers are able to redirect users to malicious domains, run external JavaScript, and steal CSRF tokens that can be used to craft CSRF attacks against admins. This issue has been fixed in version 1.5.0.	Patched by core rule	Y
CVE-2026-24034	Horilla is a free and open source Human Resource Management System (HRMS)	Horilla is a free and open source Human Resource Management System (HRMS). In versions prior to 1.5.0, a cross-site scripting vulnerability can be triggered because the extension and content-type are not checked during the profile photo update step. Version 1.5.0 fixes the issue.	Patched by core rule	Y
CVE-2021-47873	VestaCP - cross-site scripting in the IP interface configuration	VestaCP versions prior to 0.9.8-25 contain a cross-site scripting vulnerability in the IP interface configuration that allows attackers to inject malicious scripts. Attackers can exploit the 'v_interface' parameter by sending a crafted POST request to the add/ip/ endpoint with a stored XSS payload.	Patched by core rule	Y
CVE-2021-47870	GetSimple CMS My SMTP Contact Plugin 1	GetSimple CMS My SMTP Contact Plugin 1.1.2 suffers from a Stored Cross-Site Scripting (XSS) vulnerability. The plugin attempts to sanitize user input using htmlspecialchars(), but this can be bypassed by passing dangerous characters as escaped hex bytes. This allows attackers to inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary client-side code that executes in the administrator's browser when visiting a malicious page.		
CVE-2021-47858	Genexis Platinum-4410 P4410-V2-1.31A - stored cross-site scripting in the 'start_addr' parameter	Genexis Platinum-4410 P4410-V2-1.31A contains a stored cross-site scripting vulnerability in the 'start_addr' parameter of the Security Management interface. Attackers can inject malicious scripts through the start source address field that will persist and trigger for privileged users when they access the security management page.	Patched by core rule	Y
CVE-2021-47857	Moodle - persistent cross-site scripting in the calendar event subtitle field	Moodle 3.10.3 contains a persistent cross-site scripting vulnerability in the calendar event subtitle field that allows attackers to inject malicious scripts. Attackers can craft a calendar event with malicious JavaScript in the subtitle track label to execute arbitrary code when users view the event.	Patched by core rule	Y
CVE-2021-47855	Openlitespeed - stored cross-site scripting in the dashboard's Notes parameter	Openlitespeed 1.7.9 contains a stored cross-site scripting vulnerability in the dashboard's Notes parameter that allows administrators to inject malicious scripts. Attackers can craft a payload in the Notes field during listener configuration that will execute when an administrator clicks on the Default Icon.	Patched by core rule	Y
CVE-2021-47817	OpenEMR 5	OpenEMR 5.0.2.1 contains a cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript through user profile parameters. Attackers can exploit the vulnerability by crafting a malicious payload to download and execute a web shell, enabling remote command execution on the vulnerable OpenEMR instance.	Patched by core rule	Y
CVE-2026-0690	WordPress FlatPM - Ad Manager, AdSense and Custom Code - Stored XSS via the 'rank_math_description' custom field	The FlatPM â€“ Ad Manager, AdSense and Custom Code plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rank_math_description' custom field in all versions up to, and including, 3.2.2	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2026-0608	WordPress Head Meta Data - Stored XSS via the 'head-meta-data' post meta field	The Head Meta Data plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'head-meta-data' post meta field in all versions up to, and including, 20251118 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-58095	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the imagedir parameter.	Patched by core rule	Y
CVE-2025-58094	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the worklistsrc parameter.	Patched by core rule	Y
CVE-2025-58093	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the phpdir parameter.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58092	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the phpexe parameter.	Patched by core rule	Y
CVE-2025-58091	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the thumbnaildir parameter.	Patched by core rule	Y
CVE-2025-58090	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the uploaddir parameter.	Patched by core rule	Y
CVE-2025-58089	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the longtermdir parameter.	Patched by core rule	Y
CVE-2025-58088	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the archivedir parameter.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-58087	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config	Multiple reflected cross-site scripting (xss) vulnerabilities exist in the config.php functionality of MedDream PACS Premium 7.3.6.870. Specially crafted malicious URLs can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger these vulnerabilities.This vulnerability affects the status parameter.	Patched by core rule	Y
CVE-2025-58080	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyHL7App functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyHL7App functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-57881	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyEmail functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyEmail functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-57787	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyRoute functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyRoute functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-57786	MedDream PACS Premium - reflected cross-site scripting (XSS) in the notifynewstudy functionality	A reflected cross-site scripting (xss) vulnerability exists in the notifynewstudy functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-55071	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyAnonymize functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyAnonymize functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.		
CVE-2025-54861	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyCoercion functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyCoercion functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-54853	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyUser functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyUser functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-54852	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyAeTitle functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyAeTitle functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-54817	MedDream PACS Premium - reflected cross-site scripting (XSS) in the autoPurge functionality	A reflected cross-site scripting (xss) vulnerability exists in the autoPurge functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a URL to a malicious website to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-54814	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyAutopurgeFilter functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyAutopurgeFilter functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-54778	MedDream PACS Premium - reflected cross-site scripting (XSS)	A reflected cross-site scripting (xss) vulnerability exists in the existingUser	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	in the existingUser functionality	functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.		
CVE-2025-54495	MedDream PACS Premium - reflected cross-site scripting (XSS) in the emailfailedjob functionality	A reflected cross-site scripting (xss) vulnerability exists in the emailfailedjob functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-54157	MedDream PACS Premium - reflected cross-site scripting (XSS) in the encapsulatedDoc functionality	A reflected cross-site scripting (xss) vulnerability exists in the encapsulatedDoc functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-53854	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyHL7Route functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyHL7Route functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-53707	MedDream PACS Premium - reflected cross-site scripting (XSS) in the modifyTranscript functionality	A reflected cross-site scripting (xss) vulnerability exists in the modifyTranscript functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-53516	MedDream PACS Premium - reflected cross-site scripting (XSS) in the downloadZip functionality	A reflected cross-site scripting (xss) vulnerability exists in the downloadZip functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious url can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability.		
CVE-2025-46270	MedDream PACS Premium - reflected cross-site scripting (XSS) in the fetchPriorStudies functionality	A reflected cross-site scripting (xss) vulnerability exists in the fetchPriorStudies functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-44000	MedDream PACS Premium - reflected cross-site scripting (XSS) in the sendOruReport functionality	A reflected cross-site scripting (xss) vulnerability exists in the sendOruReport functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-36556	MedDream PACS Premium - reflected cross-site scripting (XSS) in the ldapUser functionality	A reflected cross-site scripting (xss) vulnerability exists in the ldapUser functionality of MedDream PACS Premium 7.3.6.870. A specially crafted malicious URL can lead to arbitrary javascript code execution. An attacker can provide a crafted URL to trigger this vulnerability.	Patched by core rule	Y
CVE-2025-15380	WordPress NotificationX - FOMO, Live Sales Notification, WooCommerce Sales Popup, GDPR, Social Proof, Announcement Banner & Floating Notification Bar - DOM-Based XSS via the 'nx-preview' POST parameter	The NotificationX â€“ FOMO, Live Sales Notification, WooCommerce Sales Popup, GDPR, Social Proof, Announcement Banner & Floating Notification Bar plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting via the 'nx-preview' POST parameter in all versions up to, and including, 3.2.0. This is due to insufficient input sanitization and output escaping when processing preview data. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute when a user visits a malicious page that auto-submits a form to the vulnerable site.	Patched by core rule	Y
CVE-2026-1045	WordPress Viet contact - Stored XSS via admin settings	The Viet contact plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.3.2 due to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.		
CVE-2026-1042	WordPress WP Hello Bar - Stored XSS via the 'digit_one' and 'digit_two' parameters	The WP Hello Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'digit_one' and 'digit_two' parameters in all versions up to, and including, 1.02 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-23852	SiYuan is a personal knowledge management system	SiYuan is a personal knowledge management system. Versions prior to 3.5.4 have a stored Cross-Site Scripting (XSS) vulnerability that allows an attacker to inject arbitrary HTML attributes into the `icon` attribute of a block via the `/api/attr/setBlockAttrs` API. The payload is later rendered in the dynamic icon feature in an unsanitized context, leading to stored XSS and, in the desktop environment, potential remote code execution (RCE). This issue bypasses the previous fix for issue `#15970` (XSS â†’ RCE via dynamic icons). Version 3.5.4 contains an updated fix.	Patched by core rule	Y
CVE-2026-23847	SiYuan is a personal knowledge management system	SiYuan is a personal knowledge management system. Versions prior to 3.5.4 are vulnerable to reflected cross-site scripting in /api/icon/getDynamicIcon due to unsanitized SVG input. The endpoint generates SVG images for text icons (type=8). The content query parameter is inserted directly into the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		SVG <text> tag without XML escaping. Since the response Content-Type is image/svg+xml, injecting unescaped tags allows breaking the XML structure and executing JavaScript. Version 3.5.4 patches the issue.]		
CVE-2026-0725	WordPress Integrate Dynamics 365 CRM - Stored XSS via admin settings	The Integrate Dynamics 365 CRM plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-8615	WordPress CubeWP - Stored XSS via the plugin's cubewp_shortcode_taxonomy shortcode	The CubeWP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cubewp_shortcode_taxonomy shortcode in all versions up to, and including, 1.1.26 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-0833	WordPress Team Section Block - Stored XSS via the plugin's block	The Team Section Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block in all versions up to, and including, 2.0.0 due to insufficient input sanitization and output escaping on user-supplied social network link URLs. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-0691	WordPress CM E-Mail Blacklist - Simple email filtering for safer registration - Stored XSS	The CM E-Mail Blacklist â€“ Simple email filtering for safer registration plugin for WordPress is vulnerable to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	via the 'black_email' parameter	Stored Cross-Site Scripting via the 'black_email' parameter in all versions up to, and including, 1.6.2. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.		
CVE-2019-25297	Poll, Survey & Quiz Maker Plugin by Opinion Stage Wordpress plugin versions prior to 19	Poll, Survey & Quiz Maker Plugin by Opinion Stage Wordpress plugin versions prior to 19.6.25 contain a stored cross-site scripting (XSS) vulnerability via multiple parameters due to insufficient input validation and output escaping. An unauthenticated attacker can inject arbitrary script into content that executes when a victim views an affected page.	Patched by core rule	Y
CVE-2026-23725	WeGIA is a web manager for charitable institutions	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the html/pet/adotantes/cadastro_adotante.php and html/pet/adotantes/informacao_adotantes.php endpoint of the WeGIA application. The application does not sanitize user-controlled input before rendering it inside the Adopters Information table, allowing persistent JavaScript injection. Any user who visits the page will have the payload executed automatically. This vulnerability is fixed in 3.6.2.	Patched by core rule	Y
CVE-2026-23724	WeGIA is a web manager for charitable institutions	WeGIA is a web manager for charitable institutions. Prior to 3.6.2, a Stored Cross-Site Scripting (XSS) vulnerability was identified in the html/atendido/cadastro_ocorrencia.php endpoint of the WeGIA application. The application does not sanitize user-controlled data before rendering it inside the â€œAtendidoâ€ selection dropdown. This vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is fixed in 3.6.2.		
CVE-2026-23722	WeGIA is a Web Manager for Charitable Institutions	WeGIA is a Web Manager for Charitable Institutions. Prior to 3.6.2, a Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the WeGIA system, specifically within the html/memorando/insere_despacho.php file. The application fails to properly sanitize or encode user-supplied input via the id_memorando GET parameter before reflecting it into the HTML source (likely inside a <script> block or an attribute). This allows unauthenticated attackers to inject arbitrary JavaScript or HTML into the context of the user's browser session. This vulnerability is fixed in 3.6.2.	Patched by core rule	Y
CVE-2026-23645	SiYuan is self-hosted, open source personal knowledge management software	SiYuan is self-hosted, open source personal knowledge management software. Prior to 3.5.4-dev2, a Stored Cross-Site Scripting (XSS) vulnerability exists in SiYuan Note. The application does not sanitize uploaded SVG files. If a user uploads and views a malicious SVG file (e.g., imported from an untrusted source), arbitrary JavaScript code is executed in the context of their authenticated session. This vulnerability is fixed in 3.5.4-dev2.	Patched by core rule	Y
CVE-2021-47844	Xmind 2020 contains a cross-site scripting vulnerability that allows attackers to inject malicious payloads into mind mapping files or cu...	Xmind 2020 contains a cross-site scripting vulnerability that allows attackers to inject malicious payloads into mind mapping files or custom headers. Attackers can craft malicious files with embedded JavaScript that execute system commands when opened, enabling remote code execution through mouse interactions or file opening.	Patched by core rule	Y
CVE-2021-47842	StudyMD 0	StudyMD 0.3.2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into markdown files. Attackers can upload crafted markdown files with embedded JavaScript payloads that execute when the file is opened,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		potentially enabling remote code execution.		
CVE-2021-47841	SnipCommand 0	SnipCommand 0.1.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious payloads into command snippets. Attackers can execute arbitrary code by embedding malicious JavaScript that triggers remote command execution through file or title inputs.	Patched by core rule	Y
CVE-2021-47840	Moeditor 0	Moeditor 0.2.0 contains a persistent cross-site scripting vulnerability that allows attackers to store malicious payloads within markdown files. Attackers can upload specially crafted markdown files with embedded JavaScript that execute when opened, potentially enabling remote code execution on the victim's system.	Patched by core rule	Y
CVE-2021-47839	Marky 0	Marky 0.0.1 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into markdown files. Attackers can upload crafted markdown files with embedded JavaScript payloads that execute when the file is opened, potentially enabling remote code execution.	Patched by core rule	Y
CVE-2021-47838	Markright 1	Markright 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to embed malicious payloads in markdown files. Attackers can upload specially crafted markdown files that execute arbitrary JavaScript when opened, potentially enabling remote code execution on the victim's system.	Patched by core rule	Y
CVE-2021-47837	Markdownify 1	Markdownify 1.2.0 contains a persistent cross-site scripting vulnerability that allows attackers to store malicious payloads within markdown files. Attackers can upload crafted markdown files with embedded scripts that execute when the file is opened, potentially enabling remote code execution.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-47836	Markdown Explorer 0	Markdown Explorer 0.1.1 contains a cross-site scripting vulnerability that allows attackers to inject malicious code through file uploads and editor inputs. Attackers can upload markdown files with embedded JavaScript payloads to execute remote commands and potentially gain system access.	Patched by core rule	Y
CVE-2021-47835	Freeter 1	Freeter 1.2.1 contains a persistent cross-site scripting vulnerability that allows attackers to store malicious payloads in custom widget titles and files. Attackers can craft malicious files with embedded scripts that execute when victims interact with the application, potentially enabling remote code execution.	Patched by core rule	Y
CVE-2021-47834	Schlix CMS 2	Schlix CMS 2.2.6-6 contains a persistent cross-site scripting vulnerability that allows authenticated users to inject malicious scripts into category titles. Attackers can create a new contact category with a script payload that will execute when the page is viewed by other users.	Patched by core rule	Y
CVE-2026-0913	WordPress User Submitted Posts - Enable Users to Submit Posts from the Front End - Stored XSS via the plugin's 'usp_access' shortcode	The User Submitted Posts â€“ Enable Users to Submit Posts from the Front End plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'usp_access' shortcode in all versions up to, and including, 20260110 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14375	WordPress RSS Aggregator - RSS Import, News Feeds, Feed to Post, and Autoblogging - Reflected XSS via the 'className' parameter	The RSS Aggregator â€“ RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the â€˜classNameâ€™ parameter in all versions up to, and including, 5.0.10 due	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2026-0916	WordPress Related Posts by Taxonomy - Stored XSS via the plugin's 'related_posts_by_tax' shortcode	The Related Posts by Taxonomy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'related_posts_by_tax' shortcode in all versions up to, and including, 2.7.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2021-47808	Cotonti Siena - stored cross-site scripting in the admin configuration panel's site title parameter	Cotonti Siena 0.9.19 contains a stored cross-site scripting vulnerability in the admin configuration panel's site title parameter. Attackers can inject malicious JavaScript code through the 'maintitle' parameter to execute scripts when administrators view the page.	Patched by core rule	Y
CVE-2021-47779	Dolibarr ERP-CRM - stored cross-site scripting in the ticket creation module	Dolibarr ERP-CRM 14.0.2 contains a stored cross-site scripting vulnerability in the ticket creation module that allows low-privilege users to inject malicious scripts. Attackers can craft a specially designed ticket message with embedded JavaScript that triggers when an administrator copies the text, potentially enabling privilege escalation.	Patched by core rule	Y
CVE-2025-70891	the user management module - stored cross-site scripting (XSS) in Phpgurukul Cyber Cafe Management System v1.0	A stored cross-site scripting (XSS) vulnerability exists in Phpgurukul Cyber Cafe Management System v1.0 within the user management module. The application does not properly sanitize or encode user-supplied input submitted via the uadd parameter in the add-users.php endpoint. An authenticated attacker can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		inject arbitrary JavaScript code that is persistently stored in the database. The malicious payload is triggered when a privileged user clicks the View button on the view-allusers.php page.		
CVE-2025-70890	the victim s browser when the affected page is accessed - stored cross-site scripting (XSS) in Cyber Cafe Management System v1.0. An authenticated attacker can inject arbitrary JavaScript code into the username parameter via the add-users.php endpoint. The injected payload is stored and executed	A stored cross-site scripting (XSS) vulnerability exists in Cyber Cafe Management System v1.0. An authenticated attacker can inject arbitrary JavaScript code into the username parameter via the add-users.php endpoint. The injected payload is stored and executed in the victim s browser when the affected page is accessed.	Patched by core rule	Y
CVE-2025-65368	SparkyFitness v0	SparkyFitness v0.15.8.2 is vulnerable to Cross Site Scripting (XSS) via user input and LLM output.	Patched by core rule	Y
CVE-2025-65349	A Stored Cross-Site Scripting (XSS) vulnerability in Web management interface in Each Italy Wireless Mini Router WIRELESS-N 300M v28K	A Stored Cross-Site Scripting (XSS) vulnerability in Web management interface in Each Italy Wireless Mini Router WIRELESS-N 300M v28K.MiniRouter.20190211 allows attackers to execute arbitrary scripts via a crafted payload due to unsanitized repeater AP SSID value when is displayed in any page at /index.htm.	Patched by core rule	Y
CVE-2025-15265	An SSR XSS exists in async hydration when attackerÃ¢â‚¬â€˜controlled keys are passed to hydratable	An SSR XSS exists in async hydration when attackerâ€˜controlled keys are passed to hydratable. The key is embedded inside a <script> block without HTMLâ€˜safe escaping, allowing </script> to terminate the script and inject arbitrary JavaScript. This enables remote script execution in users' browsers, with potential for session theft and account compromise. This issue affects Svelte: from 5.46.0 before 5.46.3.	Patched by core rule	Y
CVE-2021-47843	Tagstoo 2	Tagstoo 2.0.1 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious payloads through files or custom tags. Attackers can execute arbitrary JavaScript code to spawn system processes, access files, and perform remote code	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execution on the victim's computer.		
CVE-2021-47769	Isshue Shopping Cart - persistent cross-site scripting in title input fields across stock, customer, and invoice modules	Isshue Shopping Cart 3.5 contains a persistent cross-site scripting vulnerability in title input fields across stock, customer, and invoice modules. Attackers with privileged user accounts can inject malicious scripts that execute on preview, potentially enabling session hijacking and persistent phishing attacks.	Patched by core rule	Y
CVE-2021-47768	ImportExportTools NG - persistent HTML injection in the email export module	ImportExportTools NG 10.0.4 contains a persistent HTML injection vulnerability in the email export module that allows remote attackers to inject malicious HTML payloads. Attackers can send emails with crafted HTML in the subject that execute during HTML export, potentially compromising user data or session credentials.	Patched by core rule	Y
CVE-2025-14448	WordPress WP-Members Membership Plugin - Stored XSS via the Multiple Checkbox and Multiple Select user profile fields	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Multiple Checkbox and Multiple Select user profile fields in all versions up to, and including, 3.5.4.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-71166	Typesetter CMS - reflected cross-site scripting (XSS) in the administrative interface within the Tools Status move message handling	Typesetter CMS versions up to and including 5.1 contain a reflected cross-site scripting (XSS) vulnerability in the administrative interface within the Tools Status move message handling. The path parameter is reflected into the HTML output without proper output encoding in include/admin/Tools/Status.php. An authenticated attacker can supply crafted input containing HTML or JavaScript, resulting in arbitrary script execution in the context of an authenticated user's browser session.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-71165	Typesetter CMS - reflected cross-site scripting (XSS) in the administrative interface within the Tools Status functionality	Typesetter CMS versions up to and including 5.1 contain a reflected cross-site scripting (XSS) vulnerability in the administrative interface within the Tools Status functionality. The path parameter is reflected into the HTML response without proper output encoding in include/admin/Tools/Status.php. An authenticated attacker can supply crafted input containing HTML or JavaScript, resulting in arbitrary script execution in the context of an authenticated user's browser session.	Patched by core rule	Y
CVE-2025-71164	Typesetter CMS - reflected cross-site scripting (XSS) in the Editing component	Typesetter CMS versions up to and including 5.1 contain a reflected cross-site scripting (XSS) vulnerability in the Editing component. The images parameter (submitted as images[] in a POST request) is reflected into an HTML href attribute without proper context-aware output encoding in include/tool/Editing.php. An authenticated attacker with editing privileges can supply a JavaScript pseudo-protocol (e.g., javascript:) to trigger arbitrary JavaScript execution in the context of the victim's browser session.	Patched by core rule	Y
CVE-2025-14557	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Drupal Facebook Pixel facebo...	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Drupal Facebook Pixel facebook_pixel allows Stored XSS.This issue affects Facebook Pixel: from 7.X-1.0 through 7.X-1.1.	Patched by core rule	Y
CVE-2025-14556	Drupal (Flag) - XSS (XSS)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Drupal Flag allows Cross-Site Scripting (XSS).This issue affects Flag: from 7.X-3.0 through 7.X-3.9.	Patched by core rule	Y
CVE-2025-63644	the user profile Description field - stored cross-site scripting (XSS) in pH7Software pH7-Social-Dating-CMS 17.9.1	A stored cross-site scripting (XSS) vulnerability exists in pH7Software pH7-Social-Dating-CMS 17.9.1 in the user profile Description field.	Patched by core rule	Y
CVE-2026-0813	WordPress Short Link - Stored XSS via the 'short_link_post_title'	The Short Link plugin for WordPress is vulnerable to Stored Cross-Site Scripting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	and 'short_link_page_title' parameters	via the 'short_link_post_title' and 'short_link_page_title' parameters in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.		
CVE-2026-0812	WordPress LinkedIn SC - Stored XSS via the 'linkedin_sc_date_format', 'linkedin_sc_api_key', and 'linkedin_sc_secret_key' parameters	The LinkedIn SC plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'linkedin_sc_date_format', 'linkedin_sc_api_key', and 'linkedin_sc_secret_key' parameters in all versions up to, and including, 1.1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.	Patched by core rule	Y
CVE-2026-0741	WordPress Electric Studio Download Counter - Stored XSS via the plugin settings	The Electric Studio Download Counter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-0739	WordPress WMF Mobile Redirector - Stored XSS via the plugin settings	The WMF Mobile Redirector plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injected page.		
CVE-2026-0734	WordPress WP Allowed Hosts - Stored XSS via the 'allowed-hosts' parameter	The WP Allowed Hosts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'allowed-hosts' parameter in all versions up to, and including, 1.0.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2026-0694	WordPress SearchWiz - Stored XSS via post titles in search results	The SearchWiz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post titles in search results in all versions up to, and including, 1.0.0. This is due to the plugin using `esc_attr()` instead of `esc_html()` when outputting post titles in search results. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in post titles that will execute whenever a user performs a search and views the search results page.	Patched by core rule	Y
CVE-2026-0680	WordPress Real Post Slider Lite - Stored XSS via the plugin settings	The Real Post Slider Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin settings in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2026-0594	The List Site Contributors plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'alpha' parameter in	The List Site Contributors plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'alpha' parameter in versions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	versions up...	up to, and including, 1.1.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2025-15486	WordPress Kunze Law - Stored XSS via plugin's shortcode	The Kunze Law plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin's shortcode in all versions up to, and including, 2.1 due to the plugin fetching HTML content from a remote server and injecting it into pages without any sanitization or escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. Additional presence of a path traversal vulnerability in the shortcode name allows writing malicious HTML files to arbitrary writable locations on the server.	Patched by core rule	Y
CVE-2025-15378	WordPress AJS Footnotes - Stored XSS via the 'note_list_class' and 'popup_display_effect_in ' parameters	The AJS Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'note_list_class' and 'popup_display_effect_in' parameters in all versions up to, and including, 1.0 due to missing authorization and nonce verification on settings save, as well as insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to update plugin settings and inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-15283	WordPress Name Directory - Stored XSS via the 'name_directory_name' and 'name_directory_descript ion' parameters	The Name Directory plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name_directory_name' and 'name_directory_description ' parameters in all versions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		up to, and including, 1.30.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-15266	WordPress GeekyBot - Generate AI Content Without Prompt, Chatbot and Lead Generation - Stored XSS via the chat message field	The GeekyBot â€" Generate AI Content Without Prompt, Chatbot and Lead Generation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the chat message field in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the Chat History page.	Patched by core rule	Y
CVE-2025-15021	WordPress Gotham Block Extra Light - Stored XSS via admin settings	The Gotham Block Extra Light plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-14725	WordPress Internal Link Builder - Stored XSS via admin settings	The Internal Link Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been disabled.		
CVE-2025-14379	The Testimonials Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in version 1	The Testimonials Creator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in version 1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-13627	WordPress Makesweat - Stored XSS via the 'makesweat_clubid' setting	The Makesweat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'makesweat_clubid' setting in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12178	WordPress SpiceForms Form Builder - Stored XSS via the 'spiceforms' shortcode	The SpiceForms Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'spiceforms' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2023-54341	Webgrind 1	Webgrind 1.1 and before contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts via the file parameter in index.php. The application does not sufficiently encode user-controlled inputs, allowing attackers to execute arbitrary JavaScript in victim's browsers by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		crafting malicious URLs.		
CVE-2023-54332	Jetpack - cross-site scripting in the contact form module	Jetpack 11.4 contains a cross-site scripting vulnerability in the contact form module that allows attackers to inject malicious scripts through the post_id parameter. Attackers can craft malicious URLs with script payloads to execute arbitrary JavaScript in victims' browsers when they interact with the contact form page.	Patched by core rule	Y
CVE-2023-53985	Zstore, now referred to as Zippy CRM, 6	Zstore, now referred to as Zippy CRM, 6.5.4 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts through unvalidated input parameters. Attackers can submit crafted payloads in manual insertion points to execute arbitrary JavaScript code in victim's browser context.	Patched by core rule	Y
CVE-2022-50937	Ametys CMS - persistent cross-site scripting in the link directory's input fields for external links	Ametys CMS v4.4.1 contains a persistent cross-site scripting vulnerability in the link directory's input fields for external links. Attackers can inject malicious script code in link text and descriptions to execute persistent attacks that compromise user sessions and manipulate application modules.	Patched by core rule	Y
CVE-2022-50908	Mailhog 1	Mailhog 1.0.1 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts through email attachments. Attackers can send crafted emails with XSS payloads to execute arbitrary API calls, including message deletion and browser manipulation.	Patched by core rule	Y
CVE-2022-50906	e107 CMS 3	e107 CMS 3.2.1 contains an upload restriction bypass vulnerability that allows authenticated administrators to upload malicious SVG files through the media manager. Attackers with admin privileges can exploit this vulnerability to upload SVG files with embedded cross-site scripting (XSS) payloads that can execute arbitrary scripts when viewed.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-50905	e107 CMS version 3	e107 CMS version 3.2.1 contains multiple vulnerabilities that allow cross-site scripting (XSS) attacks. The first vulnerability is a reflected XSS that occurs in the news comment functionality when authenticated users interact with the comment form. An attacker can inject malicious JavaScript code through the URL parameter that gets executed when users click outside the comment field after typing content. The second vulnerability involves an upload restriction bypass for authenticated administrators, allowing them to upload SVG files containing malicious code through the media manager's remote URL upload feature. This results in stored XSS when the uploaded SVG files are accessed. These vulnerabilities were discovered by Hubert Wojciechowski and affect the news.php and image.php components of the CMS.	Patched by core rule	Y
CVE-2022-50896	Testa - reflected cross-site scripting in the login	Testa 3.5.1 contains a reflected cross-site scripting vulnerability in the login.php redirect parameter that allows attackers to inject malicious scripts. Attackers can craft a specially encoded payload in the redirect parameter to execute arbitrary JavaScript in victim's browser context.	Patched by core rule	Y
CVE-2022-50891	Owlfiles File Manager 12	Owlfiles File Manager 12.0.1 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through the path parameter in HTTP server endpoints. Attackers can craft URLs targeting the download and list endpoints with embedded script tags to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2021-47750	YouPHPTube <= 7	YouPHPTube <= 7.8 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts through the redirectUri parameter in the signup page. Attackers can craft special signup URLs	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with embedded script tags to execute arbitrary JavaScript in victims' browsers when they access the signup page.		
CVE-2020-36919	WPForms - cross-site scripting in the slider import search feature and tab parameter	WPForms 1.7.8 contains a cross-site scripting vulnerability in the slider import search feature and tab parameter. Attackers can inject malicious scripts through the ListTable.php endpoint to execute arbitrary JavaScript in victim's browser.	Patched by core rule	Y
CVE-2025-9427	Lemonsoft WordPress add (on) - XSS (XSS)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lemonsoft WordPress add on allows Cross-Site Scripting (XSS).This issue affects WordPress add on: 2025.7.1.	Patched by core rule	Y
CVE-2026-22813	OpenCode is an open source AI coding agent	OpenCode is an open source AI coding agent. The markdown renderer used for LLM responses will insert arbitrary HTML into the DOM. There is no sanitization with DOMPurify or even a CSP on the web interface to prevent JavaScript execution via HTML injection. This means controlling the LLM response for a chat session gets JavaScript execution on the http://localhost:4096 origin. This vulnerability is fixed in 1.1.10.	Patched by core rule	Y
CVE-2026-22804	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. From 1.7.0 to 1.9.0, Stored Cross-Site Scripting (XSS) vulnerability exists in the Termix File Manager component. The application fails to sanitize SVG file content before rendering it. This allows an attacker who has compromised a managed SSH server to plant a malicious file, which, when previewed by the Termix user, executes arbitrary JavaScript in the context of the application. The vulnerability is located in src/ui/desktop/apps/file-manager/components/FileViewer.tsx. This vulnerability is fixed in 1.10.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-22033	Label Studio is a multi-type data labeling and annotation tool	Label Studio is a multi-type data labeling and annotation tool. In 1.22.0 and earlier, a persistent stored cross-site scripting (XSS) vulnerability exists in the custom_hotkeys functionality of the application. An authenticated attacker (or one who can trick a user/administrator into updating their custom_hotkeys) can inject JavaScript code that executes in other usersâ€™ browsers when those users load any page using the templates/base.html template. Because the application exposes an API token endpoint (/api/current-user/token) to the browser and lacks robust CSRF protection on some API endpoints, the injected script may fetch the victimâ€™s API token or call token reset endpoints â€” enabling full account takeover and unauthorized API access.	Patched by core rule	Y
CVE-2025-66939	Cross Site Scripting vulnerability in 66biolinks by AltumCode v	Cross Site Scripting vulnerability in 66biolinks by AltumCode v.61.0.1 allows an attacker to execute arbitrary code via a crafted favicon file	Patched by core rule	Y
CVE-2025-12379	WordPress Shortcodes and extra features for Phlox theme - Stored XSS via a combination of the 'tag' and 'title_tag' parameters	The Shortcodes and extra features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a combination of the 'tag' and â€˜title_tagâ€™ parameters in all versions up to, and including, 2.17.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14555	WordPress Countdown Timer - Widget Countdown - Stored XSS via the plugin's 'wpdevart_countdown' shortcode	The Countdown Timer â€“ Widget Countdown plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpdevart_countdown' shortcode in all versions up to, and including, 2.7.7 due to insufficient input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-14506	WordPress ConvertForce Popup Builder - Stored XSS via the Gutenberg block's `entrance_animation` attribute	The ConvertForce Popup Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Gutenberg block's `entrance_animation` attribute in all versions up to, and including, 0.0.7. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13967	WordPress Woodpecker for WordPress - Stored XSS via the 'form_name' parameter	The Woodpecker for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'form_name' parameter of the [woodpecker-connector] shortcode in all versions up to, and including, 3.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13908	WordPress The Tooltip - Stored XSS via the plugin's 'the_tooltip' shortcode	The The Tooltip plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'the_tooltip' shortcode in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13903	WordPress PullQuote -	The PullQuote plugin for	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Stored XSS via the plugin's 'pullquote' shortcode	WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'pullquote' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	rule	
CVE-2025-13897	WordPress Client Testimonial Slider - Stored XSS via the 'aft_testimonial_meta_name' custom field in the Client Information metabox	The Client Testimonial Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'aft_testimonial_meta_name' custom field in the Client Information metabox in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected administrative page.	Patched by core rule	Y
CVE-2025-13893	WordPress Lesson Plan Book - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The Lesson Plan Book plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-13892	WordPress MG AdvancedOptions - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The MG AdvancedOptions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		into performing an action such as clicking on a link.		
CVE-2025-13862	WordPress Menu Card - Stored XSS via the `category` parameter	The Menu Card plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `category` parameter in all versions up to, and including, 0.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13854	WordPress Curved Text - Stored XSS via the 'radius' parameter	The Curved Text plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'radius' parameter of the arctext shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13852	WordPress Debt.com Business in a Box - Stored XSS via the 'configuration' parameter	The Debt.com Business in a Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'configuration' parameter of the lead_form shortcode in all versions up to, and including, 4.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13704	WordPress Autogen Headers Menu - Stored XSS via the 'head_class' parameter	The Autogen Headers Menu plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'head_class' parameter of the 'autogen_menu' shortcode in all versions up to, and including, 1.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-13701	WordPress Shabat Keeper - Reflected XSS via the $_SERVER['PHP_SELF'] parameter	The Shabat Keeper plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the $_SERVER['PHP_SELF'] parameter in all versions up to, and including, 0.4.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-11453	WordPress Header and Footer Scripts - Stored XSS via the _inpost_head_script parameter	The Header and Footer Scripts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the _inpost_head_script parameter in all versions up to, and including, 2.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13900	WordPress WP Popup Magic - Stored XSS via the 'name' parameter	The WP Popup Magic plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'name' parameter of the [wppum_end] shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13895	WordPress Top Position Google Finance - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The Top Position Google Finance plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 0.1.0 due to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2025-13853	WordPress Nearby Now Reviews - Stored XSS via the 'data_tech' parameter	The Nearby Now Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'data_tech' parameter of the nn-tech shortcode in all versions up to, and including, 5.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13729	WordPress Entry Views - Stored XSS via the plugin's 'entry-views' shortcode	The Entry Views plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'entry-views' shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-0627	WordPress AMP for WP - Stored XSS via SVG file uploads	The AMP for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file uploads in all versions up to, and including, 1.1.10. This is due to insufficient sanitization of SVG file content that only removes `<script>` tags while allowing other XSS vectors such as event handlers (onload, onerror, onmouseover), foreignObject elements, and SVG animation attributes. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts via malicious SVG file uploads that will execute whenever a user	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		views the uploaded file.		
CVE-2025-14937	WordPress Frontend Admin by DynamiApps - Stored XSS via the 'acff' parameter	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'acff' parameter in the 'frontend_admin/forms/update_field' AJAX action in all versions up to, and including, 3.28.23 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-0563	WordPress WP Google Street View (with 360Ã‚Â° virtual tour) & Google maps + Local SEO - Stored XSS via the 'wpgsv_map' shortcode	The WP Google Street View (with 360Â° virtual tour) & Google maps + Local SEO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpgsv_map' shortcode in all versions up to, and including, 1.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-15057	WordPress SlimStat Analytics - Stored XSS via the `fh` (fingerprint) parameter	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `fh` (fingerprint) parameter in all versions up to, and including, 5.3.3. This is due to insufficient input sanitization and output escaping on the fingerprint value stored in the database. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever an administrator views the Real-time Access Log report.	Patched by core rule	Y
CVE-2025-15055	WordPress SlimStat Analytics - Stored XSS via the 'notes' and 'resource' parameters	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'notes' and 'resource' parameters in all versions up to, and including, 5.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		web scripts in pages that will execute whenever an administrator accesses the Recent Custom Events report.		
CVE-2025-15019	WordPress BIALTY - Bulk Image Alt Text (Alt tag, Alt Attribute) with Yoast SEO + WooCommerce - Stored XSS via the 'bialty_cs_alt' post meta	The BIALTY - Bulk Image Alt Text (Alt tag, Alt Attribute) with Yoast SEO + WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bialty_cs_alt' post meta in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the post editor.	Patched by core rule	Y
CVE-2025-14893	WordPress IndieWeb - Stored XSS via the 'Telephone' parameter	The IndieWeb plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Telephone' parameter in all versions up to, and including, 4.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14803	The NEX-Forms WordPress plugin before 9	The NEX-Forms WordPress plugin before 9.1.8 does not sanitise and escape some of its settings. The NEX-Forms WordPress plugin before 9.1.8 can be configured in such a way that could allow subscribers to perform Stored Cross-Site Scripting.	Patched by core rule	Y
CVE-2026-0730	A flaw has been found in PHPGurukul Staff Leave Management System 1	A flaw has been found in PHPGurukul Staff Leave Management System 1.0. The affected element is the function ADD_STAFF/UPDATE_STAFF of the file /staffleave/slms/slms/admin views.py of the component SVG File Handler. Executing a manipulation of the argument profile_pic can lead to cross site scripting. The attack can be executed remotely. The exploit has been published and may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		used.		
CVE-2025-14436	WordPress Brevo for WooCommerce - Stored XSS via the 'user_connection_id' parameter	The Brevo for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the â€˜user_connection_idâ€™ parameter in all versions up to, and including, 4.0.49 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2026-22519	BuddyDev (MediaPress) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev MediaPress allows Stored XSS.This issue affects MediaPress: from n/a through 1.6.2.	Patched by core rule	Y
CVE-2026-22518	pencilwp X Addons for (Elementor) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pencilwp X Addons for Elementor allows DOM-Based XSS.This issue affects X Addons for Elementor: from n/a through 1.0.23.	Patched by core rule	Y
CVE-2026-0671	Wikimedia Foundation MediaWiki - UploadWizard (extension) - XSS (XSS)	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wikimedia Foundation MediaWiki - UploadWizard extension allows Cross-Site Scripting (XSS).This issue affects MediaWiki - UploadWizard extension: 1.45, 1.44, 1.43, 1.39.	Patched by core rule	Y
CVE-2025-61550	Cross-Site Scripting (XSS) is present on the ctl00_Content01_fieldValue parameters on the /psp/appNet/TemplateOrder/TemplatePreview	Cross-Site Scripting (XSS) is present on the ctl00_Content01_fieldValue parameters on the /psp/appNet/TemplateOrder/TemplatePreview.aspx endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34. User-supplied input is stored and later rendered in HTML pages without proper output encoding or sanitization. This allows attackers to persistently inject arbitrary JavaScript that executes in the context of other users' sessions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-61549	Cross-Site Scripting (XSS) is present on the LoginID parameter on the /PSP/app/web/reg/reg_display	Cross-Site Scripting (XSS) is present on the LoginID parameter on the /PSP/app/web/reg/reg_display.asp endpoint in edu Business Solutions Print Shop Pro WebDesk version 18.34. Unsanitized user input is reflected in HTTP responses without proper HTML encoding or escaping. This allows attackers to execute arbitrary JavaScript in the context of a victim s browser session	Patched by core rule	Y
CVE-2025-63611	Cross-Site Scripting in phpgurukul Hostel Management System v2	Cross-Site Scripting in phpgurukul Hostel Management System v2.1 user-provided complaint fields (Explain the Complaint) submitted via /register-complaint.php are stored and rendered unescaped in the admin viewer (/admin/complaint-details.php?cid=<id>). When an administrator opens the complaint, injected HTML/JavaScript executes in the admin's browser.	Patched by core rule	Y
CVE-2026-21873	NiceGUI is a Python-based UI framework	NiceGUI is a Python-based UI framework. From versions 2.22.0 to 3.4.1, an unsafe implementation in the pushstate event listener used by ui.sub_pages allows an attacker to manipulate the fragment identifier of the URL, which they can do despite being cross-site, using an iframe. This issue has been patched in version 3.5.0.	Patched by core rule	Y
CVE-2026-21872	NiceGUI is a Python-based UI framework	NiceGUI is a Python-based UI framework. From versions 2.22.0 to 3.4.1, an unsafe implementation in the click event listener used by ui.sub_pages, combined with attacker-controlled link rendering on the page, causes XSS when the user actively clicks on the link. This issue has been patched in version 3.5.0.	Patched by core rule	Y
CVE-2026-21871	NiceGUI is a Python-based UI framework	NiceGUI is a Python-based UI framework. From versions 2.13.0 to 3.4.1, there is a XSS risk in NiceGUI when developers pass attacker-controlled strings into ui.navigate.history.push() or ui.navigate.history.replace(). These helpers are documented as History API	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		wrappers for updating the browser URL without page reload. However, if the URL argument is embedded into generated JavaScript without proper escaping, a crafted payload can break out of the intended string context and execute arbitrary JavaScript in the victimâ€™s browser. Applications that do not pass untrusted input into ui.navigate.history.push/replace are not affected. This issue has been patched in version 3.5.0.		
CVE-2025-68892	gopiplus@hotmail.com Scroll rss excerpt (scroll-rss-excerpt) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in gopiplus@hotmail.com Scroll rss excerpt scroll-rss-excerpt allows Reflected XSS.This issue affects Scroll rss excerpt: from n/a through <= 5.0.	Patched by core rule	Y
CVE-2025-68891	Ryan Sutana WP App Bar (wp-app-bar) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Sutana WP App Bar wp-app-bar allows Reflected XSS.This issue affects WP App Bar: from n/a through <= 1.5.	Patched by core rule	Y
CVE-2025-68890	hands01 e-shops (e-shops-cart2) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in hands01 e-shops e-shops-cart2 allows DOM-Based XSS.This issue affects e-shops: from n/a through <= 1.0.4.	Patched by core rule	Y
CVE-2025-68889	Pinpoll Pinpoll (pinpoll) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pinpoll Pinpoll pinpoll allows Reflected XSS.This issue affects Pinpoll: from n/a through <= 4.0.0.	Patched by core rule	Y
CVE-2025-68887	CMSJunkie - WordPress Business Directory Plugins WP-BusinessDirectory (wp-businessdirectory) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CMSJunkie - WordPress Business Directory Plugins WP-BusinessDirectory wp-businessdirectory allows Reflected XSS.This issue affects WP-BusinessDirectory: from n/a through <= 3.1.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-68875	jcaruso001 Flaming Password Reset (flaming-password-reset) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in jcaruso001 Flaming Password Reset flaming-password-reset allows Stored XSS.This issue affects Flaming Password Reset: from n/a through <= 1.0.3.	Patched by core rule	Y
CVE-2025-68874	Shahjada Visitor Stats Widget (visitor-stats-widget) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shahjada Visitor Stats Widget visitor-stats-widget allows Reflected XSS.This issue affects Visitor Stats Widget: from n/a through <= 1.5.0.	Patched by core rule	Y
CVE-2025-68873	chloÃƒÂ©digital PRIMER by chloÃƒÂ©digital (primer-by-chloedigital) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in chloÃ©digital PRIMER by chloÃ©digital primer-by-chloedigital allows Reflected XSS.This issue affects PRIMER by chloÃ©digital: from n/a through <= 1.0.25.	Patched by core rule	Y
CVE-2025-68867	anibalwainstein Effect Maker (effect-maker) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in anibalwainstein Effect Maker effect-maker allows DOM-Based XSS.This issue affects Effect Maker: from n/a through <= 1.2.1.	Patched by core rule	Y
CVE-2025-67933	taskbuilder Taskbuilder (taskbuilder) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in taskbuilder Taskbuilder taskbuilder allows Reflected XSS.This issue affects Taskbuilder: from n/a through <= 4.0.9.	Patched by core rule	Y
CVE-2025-67932	purethemes Listeo Core (listeo-core) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in purethemes Listeo Core listeo-core allows Reflected XSS.This issue affects Listeo Core: from n/a through < 2.0.19.	Patched by core rule	Y
CVE-2025-67930	Vernon Systems Limited eHive Search (ehive-search) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vernon Systems Limited eHive Search ehive-search allows Reflected XSS.This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects eHive Search: from n/a through <= 2.5.0.		
CVE-2025-67927	Spencer Haws Link Whisper Free (link-whisper) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spencer Haws Link Whisper Free link-whisper allows Reflected XSS.This issue affects Link Whisper Free: from n/a through <= 0.8.8.	Patched by core rule	Y
CVE-2025-67922	ThemeGoods Grand Restaurant (grandrestaurant) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeGoods Grand Restaurant grandrestaurant allows Reflected XSS.This issue affects Grand Restaurant: from n/a through < 7.0.9.	Patched by core rule	Y
CVE-2025-67918	WofficeIO Woffice (woffice) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WofficeIO Woffice woffice allows Reflected XSS.This issue affects Woffice: from n/a through <= 5.4.30.	Patched by core rule	Y
CVE-2025-67916	Astoundify Jobify (jobify) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Astoundify Jobify jobify allows Reflected XSS.This issue affects Jobify: from n/a through <= 4.3.0.	Patched by core rule	Y
CVE-2025-27004	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Famous - Responsive Im...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup Famous - Responsive Image And Video Grid Gallery WordPress Plugin famous_grid_image_and_video_gallery allows Reflected XSS.This issue affects Famous - Responsive Image And Video Grid Gallery WordPress Plugin: from n/a through <= 1.4.	Patched by core rule	Y
CVE-2025-27002	LambertGroup CountDown With Image or Video Background (countdown-with-background) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LambertGroup CountDown With Image or Video Background countdown-with-background allows Reflected XSS.This issue affects CountDown With Image or Video Background: from n/a through <= 1.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-22725	loopus WP Virtual Assistant (VirtualAssistant) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in loopus WP Virtual Assistant VirtualAssistant allows Stored XSS.This issue affects WP Virtual Assistant: from n/a through <= 3.0.	Patched by core rule	Y
CVE-2025-14984	WordPress Gutenverse Form - Stored XSS via SVG file upload	The Gutenverse Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file upload in all versions up to, and including, 2.3.2. This is due to the plugin's framework component adding SVG to the allowed MIME types via the upload_mimes filter without implementing any sanitization of SVG file contents. This makes it possible for authenticated attackers, with Author-level access and above, to upload SVG files containing malicious JavaScript that executes when the file is viewed, leading to arbitrary JavaScript execution in victims' browsers.	Patched by core rule	Y
CVE-2025-13504	e-plugins Real Estate Pro (real-estate-pro) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins Real Estate Pro real-estate-pro allows Reflected XSS.This issue affects Real Estate Pro: from n/a through <= 2.1.4.	Patched by core rule	Y
CVE-2025-12551	e-plugins ListingHub (listinghub) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins ListingHub listinghub allows Reflected XSS.This issue affects ListingHub: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2025-14275	WordPress Jeg Elementor Kit - Stored XSS	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.0.1 due to insufficient input sanitization in the countdown widget's redirect functionality. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary JavaScript that will execute when an administrator or other user views the page containing the malicious countdown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		element.		
CVE-2019-25277	FaceSentry Access Control System - cross-site scripting in the 'msg' parameter	FaceSentry Access Control System 6.4.8 contains a cross-site scripting vulnerability in the 'msg' parameter of pluginInstall.php that allows attackers to inject malicious scripts. Attackers can exploit the unvalidated input to execute arbitrary JavaScript in victim browsers, potentially stealing authentication credentials and conducting phishing attacks.	Patched by core rule	Y
CVE-2025-66686	the admin panel - stored XSS (XSS) in Perch CMS version 3.2. An authenticated attacker with administrative privileges can inject malicious JavaScript code into the Ã¢â‚¬Å“Help button urlÃ¢â‚¬Â setting	A stored Cross-Site Scripting (XSS) vulnerability exists in Perch CMS version 3.2. An authenticated attacker with administrative privileges can inject malicious JavaScript code into the â€œHelp button urlâ€ setting within the admin panel. The injected payload is stored and executed when any authenticated user clicks the Help button, potentially leading to session hijacking, information disclosure, privilege escalation, and unauthorized administrative actions.	Patched by core rule	Y
CVE-2025-46494	Themesgrove WidgetKit (Pro) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themesgrove WidgetKit Pro allows Reflected XSS.This issue affects WidgetKit Pro: from n/a through 1.13.1.	Patched by core rule	Y
CVE-2026-0642	A vulnerability was detected in projectworlds House Rental and Property Listing 1	A vulnerability was detected in projectworlds House Rental and Property Listing 1.0. This issue affects some unknown processing of the file /app/complaint.php. The manipulation of the argument Name results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-69082	Frenify Arlo (arlo) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Frenify Arlo arlo allows Reflected XSS.This issue affects Arlo: from n/a through 6.0.3.	Patched by core rule	Y
CVE-2025-32300	Digital zoom studio DZS	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Video (Gallery) - Reflected XSS	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital zoom studio DZS Video Gallery allows Reflected XSS.This issue affects DZS Video Gallery: from n/a through 12.25.	rule	
CVE-2025-15000	WordPress Page Keys - Stored XSS via the 'page_key' parameter	The Page Keys plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the â€˜page_keyâ€™ parameter in all versions up to, and including, 1.3.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-14891	WordPress Customer Reviews for WooCommerce - Stored XSS via the 'displayName' parameter	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'displayName' parameter in all versions up to, and including, 5.93.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with customer-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. While it is possible to invoke the AJAX action without authentication, the attacker would need to know a valid form ID, which requires them to place an order. This vulnerability can be exploited by unauthenticated attackers if guest checkout is enabled. However, the form ID still needs to be obtained through placing an order.	Patched by core rule	Y
CVE-2025-14888	WordPress Simple User Meta Editor - Stored XSS via the user meta value field	The Simple User Meta Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user meta value field in all versions up to, and including, 1.0.0 due to insufficient input sanitization	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.		
CVE-2025-14887	WordPress twinklesmtp - Email Service Provider For WordPress - Stored XSS via plugin's sender settings	The twinklesmtp â€“ Email Service Provider For WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin's sender settings in all versions up to, and including, 1.03 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-14875	WordPress HBLPAY Payment Gateway for WooCommerce - Reflected XSS via the 'cusdata' parameter	The HBLPAY Payment Gateway for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the â€˜cusdataâ€™ parameter in all versions up to, and including, 5.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-14796	WordPress My Album Gallery - Stored XSS via image titles	The My Album Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via image titles in all versions up to, and including, 1.0.4. This is due to insufficient input sanitization and output escaping on the 'attachment->title' attribute. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		execute whenever a user accesses an injected page.		
CVE-2025-14626	WordPress QR Code for WooCommerce order emails, PDF invoices, packing slips - Stored XSS via the plugin's shortcode	The QR Code for WooCommerce order emails, PDF invoices, packing slips plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode in all versions up to, and including, 1.9.42 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14453	WordPress My Album Gallery - Stored XSS via the 'style_css' shortcode attribute	The My Album Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'style_css' shortcode attribute in all versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14147	WordPress Easy GitHub Gist Shortcodes - Stored XSS via the 'id' parameter	The Easy GitHub Gist Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the gist shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14145	WordPress Niche Hero | Beautifully-designed blocks in seconds - Stored XSS via the 'spacing' parameter	The Niche Hero | Beautifully-designed blocks in seconds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'spacing' parameter of the nh_row shortcode in all versions up to, and including, 1.0.5 due to insufficient input sanitization and output escaping. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-14144	WordPress Mstoic Shortcodes - Stored XSS via the 'start' parameter	The Mstoic Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'start' parameter of the ms_youtube_embeds shortcode in all versions up to, and including, 2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14131	WordPress WP Widget Changer - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The WP Widget Changer plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.2.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-14130	WordPress Post Like Dislike - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The Post Like Dislike plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-14128	WordPress Stumble! for WordPress - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The Stumble! for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 1.1.1 due to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2025-14127	WordPress Testimonial Master - Reflected XSS via the `$_SERVER['PHP_SELF']` variable	The Testimonial Master plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `$_SERVER['PHP_SELF']` variable in all versions up to, and including, 0.2.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	Patched by core rule	Y
CVE-2025-14122	WordPress AD Sliding FAQ - Stored XSS via the 'sliding_faq' shortcode	The AD Sliding FAQ plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sliding_faq' shortcode in all versions up to, and including, 2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14121	WordPress EDD Download Info - Stored XSS via the 'edd_download_info_link' shortcode	The EDD Download Info plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'edd_download_info_link' shortcode in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14118	WordPress Starred Review - Reflected XSS via the PHP_SELF variable	The Starred Review plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the PHP_SELF variable in all versions up to, and including, 1.4.2 due to insufficient input sanitization	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.		
CVE-2025-14114	WordPress 1180px Shortcodes - Stored XSS via the 'class' shortcode attribute	The 1180px Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' shortcode attribute in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14113	WordPress Viitor Button Shortcodes - Stored XSS via the 'link' shortcode attribute	The Viitor Button Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' shortcode attribute in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14112	WordPress Snillrik Restaurant - Stored XSS via the 'menu_style' shortcode attribute	The Snillrik Restaurant plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'menu_style' shortcode attribute in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14110	WordPress WP Js List Pages Shortcodes - Stored XSS via the 'class' shortcode attribute	The WP Js List Pages Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class' shortcode attribute in all versions up	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to, and including, 1.21 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-14109	WordPress AH Shortcodes - Stored XSS via the 'column' shortcode attribute	The AH Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'column' shortcode attribute in all versions up to, and including, 1.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14057	WordPress Multi-column Tag Map - Stored XSS via admin settings	The Multi-column Tag Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 17.0.39 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-14053	WordPress Wish To Go - Stored XSS via shortcode attributes	The Wish To Go plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcode attributes in all versions up to, and including, 0.5.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14028	WordPress Contact Us	The Contact Us Simple Form	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Simple Form - Stored XSS via admin settings	plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	rule	
CVE-2025-13974	WordPress Email Customizer for WooCommerce - Stored XSS via email template content	The Email Customizer for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via email template content in all versions up to, and including, 2.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in email templates that will execute when customers view transactional emails. This only affects multi-site installations and installations where unfiltered_html has been disabled.	Patched by core rule	Y
CVE-2025-13887	WordPress AI BotKit - AI Chatbot & Live Support for WordPress - Stored XSS via the 'id' parameter	The AI BotKit â€“ AI Chatbot & Live Support for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in the `ai_botkit_widget` shortcode in all versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13849	WordPress Cool YT Player - Stored XSS via the 'videoid' parameter	The Cool YT Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'videoid' parameter in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-13848	WordPress STM Gallery 1.9 - Stored XSS via the 'composicion' parameter	The STM Gallery 1.9 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'composicion' parameter in all versions up to, and including, 0.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13847	WordPress PhotoFade - Stored XSS via the 'time' parameter	The PhotoFade plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'time' parameter in all versions up to, and including, 0.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13841	WordPress Smart App Banners - Stored XSS via the 'size' and 'verticalalign' parameters of the 'app-store-download' shortcode	The Smart App Banners plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'size' and 'verticalalign' parameters of the 'app-store-download' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13667	WordPress WP Recipe Manager - Stored XSS via the 'Skill Level' input field	The WP Recipe Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Skill Level' input field in all versions up to, and including, 1.0.0 due to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.		
CVE-2025-13531	WordPress Stylish Order Form Builder - Stored XSS via the 'product_name' parameter	The Stylish Order Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'product_name' parameter in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13497	WordPress Recras WordPress - Stored XSS via the 'recrasname' shortcode attribute	The Recras WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'recrasname' shortcode attribute in all versions up to, and including, 6.4.1. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13418	WordPress Responsive Pricing Table - Stored XSS via the 'plan_icons' parameter	The Responsive Pricing Table plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'plan_icons' parameter in all versions up to, and including, 5.1.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-13369	WordPress Premmerce WooCommerce Customers Manager - Reflected XSS via the 'money_spent_from',	The Premmerce WooCommerce Customers Manager plugin for WordPress is vulnerable to Reflected Cross-Site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	'money_spent_to', 'registered_from', and 'registered_to' parameters	Scripting via the 'money_spent_from', 'money_spent_to', 'registered_from', and 'registered_to' parameters in all versions up to, and including, 1.1.14 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrator into performing an action such as clicking on a link.		
CVE-2025-31642	Dasinfomedia (WPCHURCH) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dasinfomedia WPCHURCH allows Reflected XSS.This issue affects WPCHURCH: from n/a through 2.7.0.	Patched by core rule	Y
CVE-2025-30631	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA-Team Woocommerce Sales Funnel Bu...	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AA-Team Woocommerce Sales Funnel Builder, AA-Team Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer) allows Reflected XSS.This issue affects Woocommerce Sales Funnel Builder: from n/a through 1.1; Amazon Affiliates Addon for WPBakery Page Builder (formerly Visual Composer): from n/a through 1.2.	Patched by core rule	Y
CVE-2025-69362	POSIMYTH UiChemy (uichemy) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POSIMYTH UiChemy uichemy allows Stored XSS.This issue affects UiChemy: from n/a through <= 4.4.2.	Patched by core rule	Y
CVE-2025-69360	CodexThemes TheGem Theme Elements (for WPBakery) (thegem-elements) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for WPBakery) thegem-elements allows DOM-Based XSS.This issue affects TheGem Theme Elements (for WPBakery): from n/a through <= 5.11.0.	Patched by core rule	Y
CVE-2025-69357	CodexThemes TheGem Theme Elements (for	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Elementor) (thegem-elements-elementor) - Stored XSS	Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem Theme Elements (for Elementor) thegem-elements-elementor allows Stored XSS.This issue affects TheGem Theme Elements (for Elementor): from n/a through <= 5.11.0.		
CVE-2025-69350	Themepoints Accordion (accordions-wp) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Accordion accordions-wp allows Stored XSS.This issue affects Accordion: from n/a through <= 3.0.3.	Patched by core rule	Y
CVE-2025-69335	Themepoints Team Showcase (team-showcase) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themepoints Team Showcase team-showcase allows Stored XSS.This issue affects Team Showcase: from n/a through <= 2.9.	Patched by core rule	Y
CVE-2025-69334	WPFactory Wishlist for WooCommerce (wish-list-for-woocommerce) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Wishlist for WooCommerce wish-list-for-woocommerce allows Stored XSS.This issue affects Wishlist for WooCommerce: from n/a through <= 3.3.0.	Patched by core rule	Y
CVE-2025-69085	e-plugins (JobBank) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e-plugins JobBank allows Reflected XSS.This issue affects JobBank: from n/a through 1.2.2.	Patched by core rule	Y
CVE-2025-69084	GT3 themes Photo (Gallery) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GT3 themes Photo Gallery allows Reflected XSS.This issue affects Photo Gallery: from n/a through 2.7.7.26.	Patched by core rule	Y
CVE-2024-31088	WPShop.Ru AdsPlace'r - Ad Manager, Inserter, AdSense (Ads) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPShop.Ru AdsPlace'r â€“ Ad Manager, Inserter, AdSense Ads allows DOM-Based XSS.This issue affects AdsPlace'r â€“ Ad Manager, Inserter, AdSense Ads: from	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		n/a through 1.1.5.		
CVE-2024-30547	Shazdeh Header Image Slider (header-image-slider) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Shazdeh Header Image Slider header-image-slider allows DOM-Based XSS.This issue affects Header Image Slider: from n/a through 0.3.	Patched by core rule	Y
CVE-2025-14552	WordPress MediaPress - Stored XSS via the plugin's mpp-uploader shortcode	The MediaPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's mpp-uploader shortcode in all versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-12067	WordPress Table Field Add-on for ACF and SCF - Stored XSS via the Table Cell Content	The Table Field Add-on for ACF and SCF plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Table Cell Content in all versions up to, and including, 1.3.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-4776	The Phlox theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption` HTML attribute in all versions up to, a...	The Phlox theme for WordPress is vulnerable to Stored Cross-Site Scripting via the `data-caption` HTML attribute in all versions up to, and including, 2.17.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-14120	WordPress URL Image Importer - Stored XSS via SVG File uploads	The URL Image Importer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and including, 1.0.7 due to insufficient sanitization of SVG files. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.		
CVE-2025-13746	WordPress ForumWP - Forum & Discussion Board - Stored XSS via the User's Display Name	The ForumWP â€“ Forum & Discussion Board plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the User's Display Name in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	Patched by core rule	Y
CVE-2025-65110	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs	Vega is a visualization grammar, a declarative format for creating, saving, and sharing interactive visualization designs. Prior to versions 6.1.2 and 5.6.3, applications meeting two conditions are at risk of arbitrary JavaScript code execution, even if "safe mode" expressionInterpreter is used. First, they use `vega` in an application that attaches both `vega` library and a `vega.View` instance similar to the Vega Editor to the global `window`, or has any other satisfactory function gadgets in the global scope. Second, they allow user-defined Vega `JSON` definitions (vs JSON that was is only provided through source code). This vulnerability allows for DOM XSS, potentially stored, potentially reflected, depending on how the library is being used. The vulnerability requires user interaction with the page to trigger. An attacker can exploit this issue by tricking a user into opening a malicious Vega specification. Successful exploitation allows the attacker to execute arbitrary JavaScript in the context of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		applicationâ€™s domain. This can lead to theft of sensitive information such as authentication tokens, manipulation of data displayed to the user, or execution of unauthorized actions on behalf of the victim. This exploit compromises confidentiality and integrity of impacted applications.Patched versions are available in `vega-selections@6.1.2` (requires ESM) for Vega v6 and `vega-selections@5.6.3` (no ESM needed) for Vega v5. As a workaround, do not attach `vega` or `vega.View` instances to global variables or the window as the editor used to do. This is a development-only debugging practice that should not be used in any situation where Vega/Vega-lite definitions can come from untrusted parties.		
CVE-2025-59158	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Coolify versions prior to and including v4.0.0-beta.420.6 are vulnerable to a stored cross-site scripting (XSS) attack in the project creation workflow. An authenticated user with low privileges (e.g., member role) can create a project with a maliciously crafted name containing embedded JavaScript. When an administrator later attempts to delete the project or its associated resource, the payload automatically executes in the adminâ€™s browser context. Version 4.0.0-beta.420.7 contains a patch for the issue.	Patched by core rule	Y
CVE-2025-67316	An issue in realme Internet browser v	An issue in realme Internet browser v.45.13.4.1 allows a remote attacker to execute arbitrary code via a crafted webpage in the built-in HeyTap/ColorOS browser	Patched by core rule	Y
CVE-2025-39497	Dokan Dokan (Pro) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dokan Dokan Pro allows Stored XSS.This issue affects Dokan Pro: from n/a through 3.14.5.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-53735	Corourke iPhone Webclip (Manager) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Corourke iPhone Webclip Manager allows Stored XSS.This issue affects iPhone Webclip Manager: from n/a through 0.5.	Patched by core rule	Y
CVE-2024-30461	Tumult Inc Tumult Hype (Animations) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tumult Inc Tumult Hype Animations allows DOM-Based XSS.This issue affects Tumult Hype Animations: from n/a through 1.9.11.	Patched by core rule	Y
CVE-2024-23511	POSIMYTH The Plus Addons for Elementor Page Builder (Lite) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows DOM-Based XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.3.3.	Patched by core rule	Y
CVE-2023-51513	INTINITUM FORM Geo (Controller) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in INTINITUM FORM Geo Controller allows DOM-Based XSS.This issue affects Geo Controller: from n/a through 8.5.2.	Patched by core rule	Y
CVE-2023-49186	KlbTheme Machic (Core) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in KlbTheme Machic Core allows DOM-Based XSS.This issue affects Machic Core: from n/a through 1.2.6.	Patched by core rule	Y
CVE-2026-0586	A vulnerability was detected in code-projects Online Product Reservation System 1	A vulnerability was detected in code-projects Online Product Reservation System 1.0. The affected element is an unknown function of the file handgunner-administrator/prod.php. Performing a manipulation of the argument cat results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2025-15454	A vulnerability was detected in zhanglun lettura up to 0	A vulnerability was detected in zhanglun lettura up to 0.1.22. This issue affects some unknown processing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file src/components/ArticleView/ContentRender.tsx of the component RSS Handler. The manipulation results in cross site scripting. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is assessed as difficult. The exploit is now public and may be used. The patch is identified as 67213093db9923e828a6e3fd8696a998c85da2d4. It is best practice to apply a patch to resolve this issue.		
CVE-2025-15452	A weakness has been identified in xnx3 wangmarket up to 4	A weakness has been identified in xnx3 wangmarket up to 4.9. This affects the function variableList of the file /admin/system/variableList.do of the component Backend Variable Search. Executing a manipulation of the argument Description can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15451	A security flaw has been discovered in xnx3 wangmarket up to 4	A security flaw has been discovered in xnx3 wangmarket up to 4.9. Affected by this issue is some unknown functionality of the file /admin/system/variableSave.do of the component System Variables Page. Performing a manipulation of the argument Description results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-21451	Bagisto is an open source laravel eCommerce platform	Bagisto is an open source laravel eCommerce platform. A stored Cross-Site Scripting (XSS) vulnerability exists in Bagisto prior to version 2.3.10 within the CMS page editor. Although the platform normally attempts to sanitize	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		`<script>` tags, the filtering can be bypassed by manipulating the raw HTTP POST request before submission. As a result, arbitrary JavaScript can be stored in the CMS content and executed whenever the page is viewed or edited. This exposes administrators to a high-severity risk, including complete account takeover, backend hijacking, and malicious script execution. Version 2.3.10 fixes the issue.		
CVE-2026-21432	Emlog is an open source website building system	Emlog is an open source website building system. Version 2.5.23 has a stored cross-site scripting vulnerability that can lead to account takeover, including takeover of admin accounts. As of time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2026-21431	Emlog is an open source website building system	Emlog is an open source website building system. Version 2.5.23 has a stored cross-site scripting vulnerability in the `Resource media library ` function while publishing an article. As of time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2026-21430	Emlog is an open source website building system	Emlog is an open source website building system. In version 2.5.23, article creation functionality is vulnerable to cross-site request forgery (CSRF). This can lead to a user being forced to post an article with arbitrary, attacker-controlled content. This, when combined with stored cross-site scripting, leads to account takeover. As of time of publication, no known patched versions are available.	Patched by core rule	Y
CVE-2025-15416	A vulnerability was found in xnx3 wangmarket up to 6	A vulnerability was found in xnx3 wangmarket up to 6.4. This affects an unknown function of the file /siteVar/save.do of the component Add Global Variable Handler. The manipulation of the argument Remark/Variable Value results in cross site scripting. The attack can be executed remotely. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-53235	osuthorpe Easy (Social) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in osuthorpe Easy Social allows Reflected XSS.This issue affects Easy Social: from n/a through 1.3.	Patched by core rule	Y
CVE-2025-52739	uxper (Sala) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uxper Sala allows Reflected XSS.This issue affects Sala: from n/a through 1.1.3.	Patched by core rule	Y
CVE-2025-50053	nebelhorn Blappsta Mobile App Plugin & Your native, mobile iPhone App and Android (App) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nebelhorn Blappsta Mobile App Plugin & Your native, mobile iPhone App and Android App allows Reflected XSS.This issue affects Blappsta Mobile App Plugin – Your native, mobile iPhone App and Android App: from n/a through 0.8.8.8.	Patched by core rule	Y
CVE-2025-47566	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomSounds allows Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZoomSounds allows Reflected XSS.This issue affects ZoomSounds: from n/a through 6.91.	Patched by core rule	Y
CVE-2025-23757	Proloy Chakroborty ZD Scribd (iPaper) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Proloy Chakroborty ZD Scribd iPaper allows Reflected XSS.This issue affects ZD Scribd iPaper: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23719	zckevin (ZhinaTwitterWidget) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zckevin ZhinaTwitterWidget allows Reflected XSS.This issue affects ZhinaTwitterWidget: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-23707	Matamko En (Masse) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Scripting') vulnerability in Matamko En Masse allows Reflected XSS.This issue affects En Masse: from n/a through 1.0.		
CVE-2025-23705	Terry Zielke Zielke Design Project (Gallery) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Terry Zielke Zielke Design Project Gallery allows Reflected XSS.This issue affects Zielke Design Project Gallery: from n/a through 2.5.0.	Patched by core rule	Y
CVE-2025-23667	Christopher (Churchill) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Christopher Churchill allows Reflected XSS.This issue affects custom-post-edit: from n/a through 1.0.4.	Patched by core rule	Y
CVE-2025-62989	Boxy Studio (Cooked) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Boxy Studio Cooked allows Stored XSS.This issue affects Cooked: from n/a through 1.11.2.	Patched by core rule	Y
CVE-2025-59135	eLEOPARD Behance Portfolio (Manager) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eLEOPARD Behance Portfolio Manager allows Stored XSS.This issue affects Behance Portfolio Manager: from n/a through 1.7.5.	Patched by core rule	Y
CVE-2025-49355	ikaes Accessibility (Press) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ikaes Accessibility Press allows Stored XSS.This issue affects Accessibility Press: from n/a through 1.0.2.	Patched by core rule	Y
CVE-2025-49337	janhenckens Dashboard (Beacon) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in janhenckens Dashboard Beacon allows Stored XSS.This issue affects Dashboard Beacon: from n/a through 1.2.0.	Patched by core rule	Y
CVE-2025-23608	Omar Mohamed Mohamoud LIVE (TV) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Omar Mohamed Mohamoud LIVE TV allows Reflected XSS.This issue affects LIVE	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		TV: from n/a through 1.2.		
CVE-2025-63021	codetipi Valenti (Engine) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codetipi Valenti Engine allows DOM-Based XSS.This issue affects Valenti Engine: from n/a through 1.0.3.	Patched by core rule	Y
CVE-2025-63020	Wayne Allen Postie (postie) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wayne Allen Postie postie allows Stored XSS.This issue affects Postie: from n/a through 1.9.73.	Patched by core rule	Y
CVE-2025-62750	Filipe Seabra WooCommerce (Parcelas) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Filipe Seabra WooCommerce Parcelas allows DOM-Based XSS.This issue affects WooCommerce Parcelas: from n/a through 1.3.5.	Patched by core rule	Y
CVE-2025-62149	SaifuMak Add Custom (Codes) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SaifuMak Add Custom Codes allows Stored XSS.This issue affects Add Custom Codes: from n/a through 4.80.	Patched by core rule	Y
CVE-2025-62142	nicashmu Cincopa video and media (plugin) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in nicashmu Cincopa video and media plugin allows Stored XSS.This issue affects Cincopa video and media plug-in: from n/a through 1.163.	Patched by core rule	Y
CVE-2025-62140	Plainware Locatoraid Store (Locator) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plainware Locatoraid Store Locator allows Stored XSS.This issue affects Locatoraid Store Locator: from n/a through 3.9.65.	Patched by core rule	Y
CVE-2025-62124	Soli WP Post (Signature) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Soli WP Post Signature allows Stored XSS.This issue affects WP Post Signature: from n/a through 0.4.1.	Patched by core rule	Y
CVE-2025-62121	Imran Emu Logo Slider ,	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Logo Carousel , Logo showcase , Client (Logo) - Stored XSS	Input During Web Page Generation ('Cross-site Scripting') vulnerability in Imran Emu Logo Slider , Logo Carousel , Logo showcase , Client Logo allows Stored XSS.This issue affects Logo Slider , Logo Carousel , Logo showcase , Client Logo: from n/a through 1.8.1.	rule	
CVE-2025-62119	ViitorCloud Technologies Pvt Ltd Add Featured Image Custom (Link) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ViitorCloud Technologies Pvt Ltd Add Featured Image Custom Link allows DOM-Based XSS.This issue affects Add Featured Image Custom Link: from n/a through 2.0.0.	Patched by core rule	Y
CVE-2025-62097	SEOthemes SEO (Slider) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SEOthemes SEO Slider allows DOM-Based XSS.This issue affects SEO Slider: from n/a through 1.1.1.	Patched by core rule	Y
CVE-2025-62096	WPFactory Maximum Products per User for (WooCommerce) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFactory Maximum Products per User for WooCommerce allows Stored XSS.This issue affects Maximum Products per User for WooCommerce: from n/a through 4.4.2.	Patched by core rule	Y
CVE-2025-62095	Neilgee Bootstrap (Modals) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Neilgee Bootstrap Modals allows Stored XSS.This issue affects Bootstrap Modals: from n/a through 1.3.2.	Patched by core rule	Y
CVE-2025-62990	Livemesh Livemesh Addons for Beaver Builder (addons-for-beaver-builder) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for Beaver Builder addons-for-beaver-builder allows Stored XSS.This issue affects Livemesh Addons for Beaver Builder: from n/a through 3.9.2.	Patched by core rule	Y
CVE-2025-62744	Chris Steman Page Title (Splitter) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chris Steman Page Title Splitter allows Stored	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		XSS.This issue affects Page Title Splitter: from n/a through 2.5.9.		
CVE-2025-62743	zookatron MyBookTable (Bookstore) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in zookatron MyBookTable Bookstore allows Stored XSS.This issue affects MyBookTable Bookstore: from n/a through 3.5.5.	Patched by core rule	Y
CVE-2025-62742	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Curator	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Curator.Io allows Stored XSS.This issue affects Curator.Io: from n/a through 1.9.5.	Patched by core rule	Y
CVE-2025-62125	Anshul Gangrade Custom Background Changer (custom-background-changer) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Anshul Gangrade Custom Background Changer custom-background-changer allows Stored XSS.This issue affects Custom Background Changer: from n/a through 3.0.	Patched by core rule	Y
CVE-2025-62118	kcseopro AdWords Conversion Tracking (Code) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kcseopro AdWords Conversion Tracking Code allows Stored XSS.This issue affects AdWords Conversion Tracking Code: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-62111	Webvitaly Extra (Shortcodes) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webvitaly Extra Shortcodes allows Stored XSS.This issue affects Extra Shortcodes: from n/a through 2.2.	Patched by core rule	Y
CVE-2025-49357	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Audiomack allows Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Audiomack allows Stored XSS.This issue affects Audiomack: from n/a through 1.4.8.	Patched by core rule	Y
CVE-2025-63032	ThinkUpThemes (Consulting) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThinkUpThemes Consulting allows Stored XSS.This issue affects Consulting: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through 1.5.0.		
CVE-2025-62991	ThinkUpThemes (Minamaze) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThinkUpThemes Minamaze allows Stored XSS.This issue affects Minamaze: from n/a through 1.10.1.	Patched by core rule	Y
CVE-2025-62757	WebMan Design | Oliver Juhas WebMan (Amplifier) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebMan Design | Oliver Juhas WebMan Amplifier allows DOM-Based XSS.This issue affects WebMan Amplifier: from n/a through 1.5.12.	Patched by core rule	Y
CVE-2025-62756	lvaudore The (Moneytizer) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in lvaudore The Moneytizer allows DOM-Based XSS.This issue affects The Moneytizer: from n/a through 10.0.6.	Patched by core rule	Y
CVE-2025-62752	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kalender	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in kalender.Digital Calendar.Online / Kalender.Digital allows DOM-Based XSS.This issue affects Calendar.Online / Kalender.Digital: from n/a through 1.0.11.	Patched by core rule	Y
CVE-2025-62749	Bainternet User Specific (Content) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bainternet User Specific Content allows DOM-Based XSS.This issue affects User Specific Content: from n/a through 1.0.6.	Patched by core rule	Y
CVE-2025-62748	Genetech Products Web and WooCommerce Addons for WPBakery (Builder) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Genetech Products Web and WooCommerce Addons for WPBakery Builder allows DOM-Based XSS.This issue affects Web and WooCommerce Addons for WPBakery Builder: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-62135	landwire Responsive Block (Control) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Scripting') vulnerability in landwire Responsive Block Control allows DOM-Based XSS.This issue affects Responsive Block Control: from n/a through 1.2.9.		
CVE-2025-49358	Ruhul Amin Content (Fetcher) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ruhul Amin Content Fetcher allows DOM-Based XSS.This issue affects Content Fetcher: from n/a through 1.1.	Patched by core rule	Y
CVE-2025-63005	Tomas WordPress (Tooltips) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tomas WordPress Tooltips allows Stored XSS.This issue affects WordPress Tooltips: from n/a through 10.7.9.	Patched by core rule	Y
CVE-2025-63000	WP for church Sermon (Manager) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP for church Sermon Manager allows Stored XSS.This issue affects Sermon Manager: from n/a through 2.30.0.	Patched by core rule	Y
CVE-2025-62761	BasePress Knowledge Base documentation & wiki plugin - (BasePress) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BasePress Knowledge Base documentation & wiki plugin â€“ BasePress allows Stored XSS.This issue affects Knowledge Base documentation & wiki plugin â€“ BasePress: from n/a through 2.17.0.1.	Patched by core rule	Y
CVE-2025-62760	BuddyDev BuddyPress Activity (Shortcode) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BuddyDev BuddyPress Activity Shortcode allows Stored XSS.This issue affects BuddyPress Activity Shortcode: from n/a through 1.1.8.	Patched by core rule	Y
CVE-2025-62759	Justin Tadlock (Series) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Justin Tadlock Series allows Stored XSS.This issue affects Series: from n/a through 2.0.1.	Patched by core rule	Y
CVE-2025-62758	Funnelforms Funnelforms (Free) - DOM-Based XSS	Improper Neutralization of Input During Web Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Generation ('Cross-site Scripting') vulnerability in Funnelforms Funnelforms Free allows DOM-Based XSS.This issue affects Funnelforms Free: from n/a through 3.8.		
CVE-2025-62146	Maksym Marko MX Time Zone (Clocks) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maksym Marko MX Time Zone Clocks allows Stored XSS.This issue affects MX Time Zone Clocks: from n/a through 5.1.1.	Patched by core rule	Y
CVE-2025-62137	Shuttlethemes (Shuttle) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shuttlethemes Shuttle allows Stored XSS.This issue affects Shuttle: from n/a through 1.5.0.	Patched by core rule	Y
CVE-2025-62136	ThinkUpThemes (Melos) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThinkUpThemes Melos allows Stored XSS.This issue affects Melos: from n/a through 1.6.0.	Patched by core rule	Y
CVE-2025-15374	A vulnerability was detected in EyouCMS up to 1	A vulnerability was detected in EyouCMS up to 1.7.7. The affected element is an unknown function of the file application/home/model/Ask.php of the component Ask Module. Performing manipulation of the argument content results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used. The vendor is "[a]cknowledging the existence of the vulnerability, we have completed the fix and will release a new version, v1.7.8".	Patched by core rule	Y
CVE-2025-15372	A weakness has been identified in youlaitech vue3-element-admin up to 3	A weakness has been identified in youlaitech vue3-element-admin up to 3.4.0. This issue affects some unknown processing of the file src/views/system/notice/index.vue of the component Notice Handler. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-15223	A vulnerability was found in Philipinho Simple-PHP-Blog up to 94b5d3e57308bce5dfbc44c3edafa9811893d958	A vulnerability was found in Philipinho Simple-PHP-Blog up to 94b5d3e57308bce5dfbc44c3edafa9811893d958. Impacted is an unknown function of the file /login.php. Performing manipulation of the argument Username results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure and makes clear that the product is "[f]or educational purposes only".	Patched by core rule	Y
CVE-2022-50787	SOUND4 IMPACT/FIRST/PULSE/Eco - unauthenticated stored cross-site scripting in the username parameter	SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x contains an unauthenticated stored cross-site scripting vulnerability in the username parameter that allows attackers to inject malicious scripts. Attackers can exploit the unvalidated username input to execute arbitrary HTML and JavaScript code in victim browser sessions without authentication.	Patched by core rule	Y
CVE-2025-66823	TrueConf server (field) - an attacker to inject arbitrary HTML in the Create/Edit conference functionality	An HTML Injection vulnerability in TrueConf server 5.5.2.10813 in the conference description field allows an attacker to inject arbitrary HTML in the Create/Edit conference functionality. The payload will be triggered when the victim opens the Conference Info page ([conference url]/info).	Patched by core rule	Y
CVE-2025-66824	the Create/Edit Conference functionality in TrueConf Server - Stored XSS (XSS) in the Meeting location field	A Stored Cross-Site Scripting (XSS) vulnerability exists in the Meeting location field of the Create/Edit Conference functionality in TrueConf Server v5.5.2.10813. The injected payload is stored via the meeting_room	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter and executed when users visit the Conference Info page, allowing attackers to achieve full Account Takeover (ATO). This issue is caused by improper sanitization of user-supplied input in the meeting_room field.		
CVE-2025-66103	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Revmakx WPCal	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Revmakx WPCal.Io allows DOM-Based XSS.This issue affects WPCal.Io: from n/a through 0.9.5.9.	Patched by core rule	Y
CVE-2025-66094	Yada Wiki (yada-wiki) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yada Wiki yada-wiki allows Stored XSS.This issue affects Yada Wiki: from n/a through 3.5.	Patched by core rule	Y
CVE-2025-64190	8theme.Com XStore (Core) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 8theme.Com XStore Core allows DOM-Based XSS.This issue affects XStore Core: from n/a before 5.6.	Patched by core rule	Y
CVE-2025-63027	Webcreations907 WBC907 (Core) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webcreations907 WBC907 Core allows Stored XSS.This issue affects WBC907 Core: from n/a through 3.4.1.	Patched by core rule	Y
CVE-2025-62746	CodeFlavors Featured Video for WordPress & (VideographyWP) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeFlavors Featured Video for WordPress & VideographyWP allows Stored XSS.This issue affects Featured Video for WordPress & VideographyWP: from n/a through 1.0.18.	Patched by core rule	Y
CVE-2025-69092	WPDeveloper Essential Addons for Elementor (essential-addons-for-elementor-lite) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor essential-addons-for-elementor-lite allows DOM-Based XSS.This issue affects Essential Addons for Elementor: from n/a through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		<= 6.5.3.		
CVE-2025-69089	autolistings Auto Listings (auto-listings) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in autolistings Auto Listings auto-listings allows Stored XSS.This issue affects Auto Listings: from n/a through <= 2.7.1.	Patched by core rule	Y
CVE-2025-69088	Vidish Combo Offers WooCommerce (woo-combo-offers) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Vidish Combo Offers WooCommerce woo-combo-offers allows DOM-Based XSS.This issue affects Combo Offers WooCommerce: from n/a through <= 4.2.	Patched by core rule	Y
CVE-2025-69033	A WP Life Blog Filter (blog-filter) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in A WP Life Blog Filter blog-filter allows DOM-Based XSS.This issue affects Blog Filter: from n/a through <= 1.7.3.	Patched by core rule	Y
CVE-2025-69020	Tribulant Software Newsletters (newsletters-lite) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tribulant Software Newsletters newsletters-lite allows Stored XSS.This issue affects Newsletters: from n/a through <= 4.12.	Patched by core rule	Y
CVE-2025-69019	FlippingBook FlippingBook (flippingbook) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FlippingBook FlippingBook flippingbook allows DOM-Based XSS.This issue affects FlippingBook: from n/a through <= 2.0.1.	Patched by core rule	Y
CVE-2025-69018	Shamalli Web Directory Free (web-directory-free) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shamalli Web Directory Free web-directory-free allows DOM-Based XSS.This issue affects Web Directory Free: from n/a through <= 1.7.12.	Patched by core rule	Y
CVE-2025-69017	Magnigenie RestroPress (restropress) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magnigenie RestroPress restropress allows Stored XSS.This issue affects RestroPress: from n/a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		through <= 3.2.4.2.		
CVE-2025-69008	Inboxify Inboxify Sign Up Form (inboxify-sign-up-form) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Inboxify Inboxify Sign Up Form inboxify-sign-up-form allows Stored XSS.This issue affects Inboxify Sign Up Form: from n/a through <= 1.0.4.	Patched by core rule	Y
CVE-2025-69007	OTWthemes Popping Sidebars and Widgets Light (popping-sidebars-and-widgets-light) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OTWthemes Popping Sidebars and Widgets Light popping-sidebars-and-widgets-light allows Stored XSS.This issue affects Popping Sidebars and Widgets Light: from n/a through <= 1.27.	Patched by core rule	Y
CVE-2025-69006	Atte Moisio AM Events (am-events) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Atte Moisio AM Events am-events allows Stored XSS.This issue affects AM Events: from n/a through <= 1.13.1.	Patched by core rule	Y
CVE-2025-68992	xenioushk BWL Knowledge Base Manager (bwl-kb-manager) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xenioushk BWL Knowledge Base Manager bwl-kb-manager allows Stored XSS.This issue affects BWL Knowledge Base Manager: from n/a through <= 1.6.3.	Patched by core rule	Y
CVE-2025-68991	xenioushk BWL Pro Voting Manager (bwl-pro-voting-manager) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in xenioushk BWL Pro Voting Manager bwl-pro-voting-manager allows DOM-Based XSS.This issue affects BWL Pro Voting Manager: from n/a through <= 1.4.9.	Patched by core rule	Y
CVE-2025-68978	designthemes DesignThemes Core (designthemes-core) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes DesignThemes Core designthemes-core allows DOM-Based XSS.This issue affects DesignThemes Core: from n/a through <= 1.6.	Patched by core rule	Y
CVE-2025-68977	designthemes	Improper Neutralization of	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	DesignThemes Portfolio Addon (designthemes-portfolio-addon) - DOM-Based XSS	Input During Web Page Generation ('Cross-site Scripting') vulnerability in designthemes DesignThemes Portfolio Addon designthemes-portfolio-addon allows DOM-Based XSS.This issue affects DesignThemes Portfolio Addon: from n/a through <= 1.5.	rule	
CVE-2025-15221	A flaw has been found in SohuTV CacheCloud up to 3	A flaw has been found in SohuTV CacheCloud up to 3.2.0. This vulnerability affects the function index of the file src/main/java/com/sohu/cache/web/controller/AppDataMigrateController.java. This manipulation causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15220	A vulnerability was detected in SohuTV CacheCloud up to 3	A vulnerability was detected in SohuTV CacheCloud up to 3.2.0. This affects the function init of the file src/main/java/com/sohu/cache/web/controller/LoginController.java. The manipulation results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15219	A security vulnerability has been detected in SohuTV CacheCloud up to 3	A security vulnerability has been detected in SohuTV CacheCloud up to 3.2.0. Affected by this issue is the function doMachineList/doPodList of the file src/main/java/com/sohu/cache/web/controller/MachineManageController.java. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15214	A vulnerability was found in Campcodes Park	A vulnerability was found in Campcodes Park Ticketing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Ticketing System 1	System 1.0. The impacted element is the function save_pricing of the file admin_class.php. The manipulation of the argument name/ride results in cross site scripting. The attack may be performed from remote. The exploit has been made public and could be used.		
CVE-2025-68499	Crocoblock (JetTabs) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetTabs allows DOM-Based XSS.This issue affects JetTabs: from n/a through 2.2.12.	Patched by core rule	Y
CVE-2025-23554	Jakub Glos Off Page (SEO) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jakub Glos Off Page SEO allows Reflected XSS.This issue affects Off Page SEO: from n/a through 3.0.3.	Patched by core rule	Y
CVE-2025-23550	Kemal YAZICI Product (Puller) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kemal YAZICI Product Puller allows Reflected XSS.This issue affects Product Puller: from n/a through 1.5.1.	Patched by core rule	Y
CVE-2025-23469	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sleekplan allows Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sleekplan allows Reflected XSS.This issue affects Sleekplan: from n/a through 0.2.0.	Patched by core rule	Y
CVE-2025-23458	Rakessh Ads24 (Lite) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rakessh Ads24 Lite allows Reflected XSS.This issue affects Ads24 Lite: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-68607	Hiroaki Miyashita Custom Field (Template) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hiroaki Miyashita Custom Field Template allows Stored XSS.This issue affects Custom Field Template: from n/a through 2.7.5.	Patched by core rule	Y
CVE-2025-68504	Crocoblock (JetSearch) - DOM-Based XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Crocoblock JetSearch allows DOM-Based XSS.This issue affects JetSearch: from n/a through 3.5.16.		
CVE-2025-15204	A vulnerability was determined in SohuTV CacheCloud up to 3	A vulnerability was determined in SohuTV CacheCloud up to 3.2.0. Affected is the function doQuartzList of the file src/main/java/com/sohu/cache/web/controller/QuartzManageController.java. Executing manipulation can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15203	A vulnerability was found in SohuTV CacheCloud up to 3	A vulnerability was found in SohuTV CacheCloud up to 3.2.0. This impacts the function index of the file src/main/java/com/sohu/cache/web/controller/ResourceController.java. Performing manipulation results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15202	A vulnerability has been found in SohuTV CacheCloud up to 3	A vulnerability has been found in SohuTV CacheCloud up to 3.2.0. This affects the function taskQueueList of the file src/main/java/com/sohu/cache/web/controller/TaskController.java. Such manipulation leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15201	A flaw has been found in SohuTV CacheCloud up to 3	A flaw has been found in SohuTV CacheCloud up to 3.2.0. The impacted element is the function redirectNoPower of the file src/main/java/com/sohu/cache/web/controller/WebResourceController.java. This manipulation causes cross	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2025-15200	A vulnerability was detected in SohuTV CacheCloud up to 3	A vulnerability was detected in SohuTV CacheCloud up to 3.2.0. The affected element is the function getExceptionStatisticsByClient/getCommandStatisticsByClient/doIndex of the file src/main/java/com/sohu/cache/web/controller/AppClientDataShowController.java. The manipulation results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-68868	Codeaffairs Wp Text Slider (Widget) - Stored XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codeaffairs Wp Text Slider Widget allows Stored XSS.This issue affects Wp Text Slider Widget: from n/a through 1.0.	Patched by core rule	Y
CVE-2025-68879	Councilsoft Content Grid (Slider) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Councilsoft Content Grid Slider allows Reflected XSS.This issue affects Content Grid Slider: from n/a through 1.5.	Patched by core rule	Y
CVE-2025-68878	Prasadkirpekar Advanced Custom (CSS) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Prasadkirpekar Advanced Custom CSS allows Reflected XSS.This issue affects Advanced Custom CSS: from n/a through 1.1.0.	Patched by core rule	Y
CVE-2025-68876	INVELITY Invelity SPS (connect) - Reflected XSS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in INVELITY Invelity SPS connect allows Reflected XSS.This issue affects Invelity SPS connect: from n/a through 1.0.8.	Patched by core rule	Y
CVE-2025-65442	DOM-based Cross-Site	DOM-based Cross-Site	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scripting (XSS) vulnerability in 201206030 novel V3	Scripting (XSS) vulnerability in 201206030 novel V3.5.0 allows remote attackers to execute arbitrary JavaScript code or disclose sensitive information (e.g., user session cookies) via a crafted "wvstest" parameter in the URL or malicious script injection into window.localStorage. The vulnerability arises from insufficient validation and encoding of user-controllable data in the book comment module: unfiltered user input is stored in the backend database (book_comment table, commentContent field) and returned via API, then rendered directly into the page DOM via Vue 3's v-html directive without sanitization. Even if modern browsers' built-in XSS filters block pop-up alerts, attackers can use concealed payloads to bypass interception and achieve actual harm.	rule	
CVE-2025-15188	A vulnerability was determined in Campcodes Complete Online Beauty Parlor Management System 1	A vulnerability was determined in Campcodes Complete Online Beauty Parlor Management System 1.0. This vulnerability affects unknown code of the file /admin/search-invoices.php. Executing manipulation of the argument searchdata can lead to cross site scripting. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2025-15175	A vulnerability was detected in SohuTV CacheCloud up to 3	A vulnerability was detected in SohuTV CacheCloud up to 3.2.0. Affected by this issue is the function doAppList/appCommandAnalysis of the file src/main/java/com/sohu/cache/web/controller/AppController.java. Performing manipulation results in cross site scripting. It is possible to initiate the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15174	A security vulnerability has been detected in	A security vulnerability has been detected in SohuTV	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	SohuTV CacheCloud up to 3	CacheCloud up to 3.2.0. Affected by this vulnerability is the function doAppAuditList of the file src/main/java/com/sohu/cache/web/controller/AppManageController.java. Such manipulation leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2025-15173	A weakness has been identified in SohuTV CacheCloud up to 3	A weakness has been identified in SohuTV CacheCloud up to 3.2.0. Affected is the function advancedAnalysis of the file src/main/java/com/sohu/cache/web/controller/InstanceController.java. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15172	A security flaw has been discovered in SohuTV CacheCloud up to 3	A security flaw has been discovered in SohuTV CacheCloud up to 3.2.0. This impacts the function preview of the file src/main/java/com/sohu/cache/web/controller/RedisConfigTemplateController.java. The manipulation results in cross site scripting. The attack can be executed remotely. The exploit has been released to the public and may be exploited. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15171	A vulnerability was identified in SohuTV CacheCloud up to 3	A vulnerability was identified in SohuTV CacheCloud up to 3.2.0. This affects the function index of the file src/main/java/com/sohu/cache/web/controller/ServerController.java. The manipulation leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The project was		

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		informed of the problem early through an issue report but has not responded yet.		
CVE-2025-15170	A security vulnerability has been detected in Advaya Softech GEMS ERP Portal up to 2	A security vulnerability has been detected in Advaya Softech GEMS ERP Portal up to 2.1. This affects an unknown part of the file /home.jsp?isError=true of the component Error Message Handler. The manipulation of the argument Message leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2025-15146	A vulnerability was detected in SohuTV CacheCloud up to 3	A vulnerability was detected in SohuTV CacheCloud up to 3.2.0. This impacts the function doUserList of the file src/main/java/com/sohu/cache/web/controller/UserManageController.java. Performing manipulation results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15145	A security vulnerability has been detected in SohuTV CacheCloud up to 3	A security vulnerability has been detected in SohuTV CacheCloud up to 3.2.0. This affects the function doTotalList of the file src/main/java/com/sohu/cache/web/controller/TotalManageController.java. Such manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-15144	A weakness has been identified in dayrui XunRuiCMS up to 4	A weakness has been identified in dayrui XunRuiCMS up to 4.7.1. The impacted element is the function dr_show_error/dr_exit_msg of the file /dayrui/Fcms/Init.php of the component JSONP Callback Handler. This manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument callback causes cross site scripting. The attack can be initiated remotely. The exploit has been made available to the public and could be exploited. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-68927	Libredesk is a self-hosted customer support desk	Libredesk is a self-hosted customer support desk. Prior to version 0.8.6-beta, LibreDesk is vulnerable to stored HTML injection in the contact notes feature. When adding notes via POST /api/v1/contacts/{id}/notes, the backend automatically wraps user input in <p> tags. However, by intercepting the request and removing the <p> tag, an attacker can inject arbitrary HTML elements such as forms and images, which are then stored and rendered without proper sanitization. This can lead to phishing, CSRF-style forced actions, and UI redress attacks. This issue has been patched in version 0.8.6-beta.	Patched by core rule	Y
CVE-2025-67349	A cross-site scripting (XSS) vulnerability was identified in FluentCMS 1	A cross-site scripting (XSS) vulnerability was identified in FluentCMS 1.2.3. After logging in as an admin and navigating to the "Add Page" function, the application fails to properly sanitize input in the <head> section, allowing remote attackers to inject arbitrary script tags.	Patched by core rule	Y
CVE-2025-15094	A weakness has been identified in sunkaifei FlyCMS up to abbaa5a8daefb146ad4d61027035026b052cb414	A weakness has been identified in sunkaifei FlyCMS up to abbaa5a8daefb146ad4d61027035026b052cb414. The impacted element is the function userLogin of the file src/main/java/com/flycms/web/front/UserController.java of the component User Login. Executing manipulation of the argument redirectUrl can lead to cross site scripting. The attack can be launched remotely. The exploit has been made available to the public and could be exploited. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		project was informed of the problem early through an issue report but has not responded yet.		

INDUSFACE™

Indusface is a leading application security SaaS company, securing over 6,500 customers across 95 countries with its award-winning platform. Backed by leading institutional investors, Indusface is a category leader in cloud WAAP, with repeated recognition from top analysts and industry platforms including Gartner, Forrester, GigaOm, and G2.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

Gartner Peer Insights Customers' Choice 2024™

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 4 consecutive years

A Customers' Choice from 2022 to 2024 Gartner® Peer Insights™

CONTACT US - +91 265 6133021 | +1 866 537 8234