



Monthly Zero-Day Vulnerability Coverage Bulletin

March 2022

Total Zero-Day Vulnerabilities Found: 72

Command Injection	CSRF	Local File Inclusion	Remote Code Execution	SQL Injection	Cross - Site Scripting	XML External Entity
7	8	19	1	19	15	3

Zero-Day vulnerabilities protected through core rules	70
Zero-Day vulnerabilities protected through custom rules	2 *
Zero-Day vulnerabilities for which protection cannot be determined	0 **
Zero-Day vulnerabilities found by Indusface WAS	63

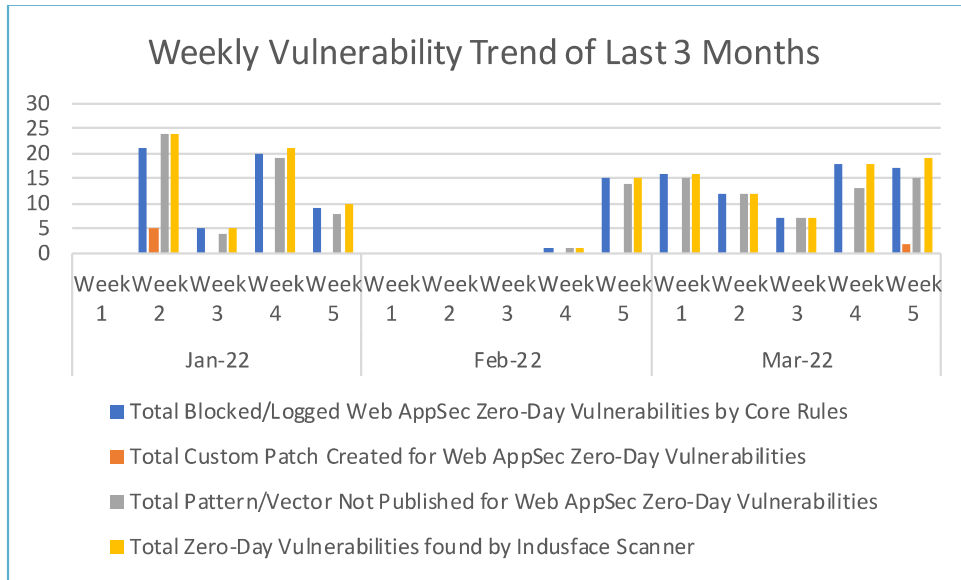
* To enable custom rules, please contact support@indusface.com

** Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.



Vulnerability Trend:

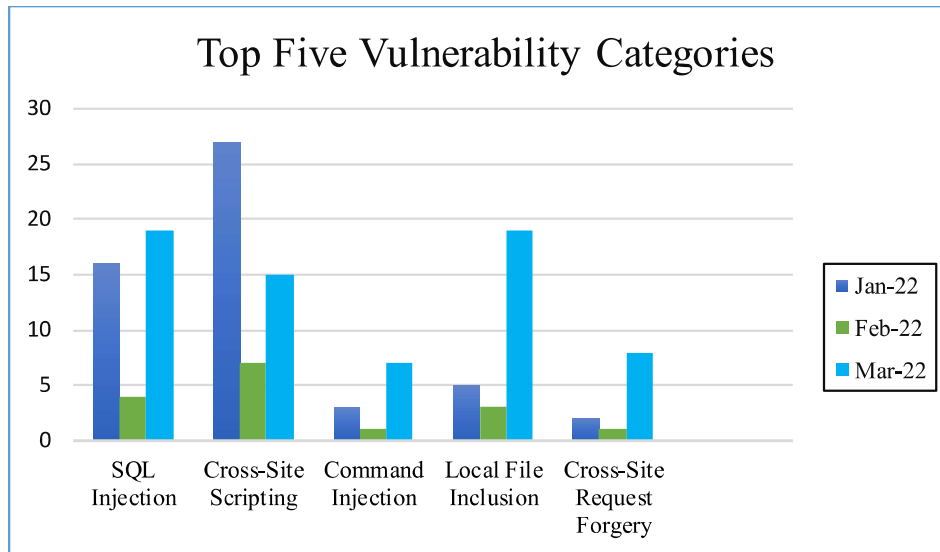
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.



25% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

75% of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

75% of the zero-day vulnerabilities were reported by **Indusface Scanner** in the last quarter



Note: Our Sig-Dev team constantly monitors the security landscape and leading security websites to identify any new vulnerabilities identified/published and monitors/updates rules to ensure round-the-clock protection for customer sites.

Vulnerability Details:

S.no	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Command Injection	CVE-2022-25018	Pluxml 5.8.7 code injection	A vulnerability was found inPluxml 5.8.7. It has been rated as critical. This issue affects an unknown functionality. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		CVE-2021-41282	pfSense 2.5.2 sed diag_routes.php os command injection	A vulnerability was found in pfSense 2.5.2. It has been declared critical. Affected by this vulnerability is an unknown part of the file. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Command Injection attack.



CVE-2022-25578	taocms 3.0.2 .htaccess code injection (ID 28)	A vulnerability classified as critical has been found in taocms 3.0.2. This affects an unknown part of the file. The manipulation with an unknown input led to privilege escalation. The attack can only be done within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
CVE-2022-25581	Classcms up to 2.5 TXT File Upload \class\classupload code injection	A vulnerability classified as critical was found in Classcms up to 2.5. The manipulation with an unknown input led to privilege escalation. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
CVE-2022-24237	Snapt Aria 12.8 snaptPowered2 command injection	A vulnerability, which was classified as critical, has been found in Snapt Aria 12.8. This issue affects some unknown processing of the component. The manipulation with an unknown input led to privilege escalation. The attack can only be done within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
CVE-2022-27811	GNOME OCRFeeder up to 0.8.3 Filename os command injection	A vulnerability, which was classified as critical, was found in GNOME OCRFeeder up to 0.8.3. This affects an unknown part of the component. The manipulation with an unknown input led to privilege escalation. The attack needs to be initiated within	Protected by core rules.	Detected by the scanner as the Command Injection attack.



				the local network. There is no exploit available. It is recommended to upgrade the affected component.		
		CVE-2022-27078	Tenda M3 1.10 /goform/setAdlnfoDetail command injection	A vulnerability has been found in Tenda M3 1.10 and classified as critical. Affected by this vulnerability is an unknown functionality of the file. The manipulation with an unknown input led to privilege escalation. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
2	Cross-Site Request Forgery	CVE-2021-44321	Mini-Inventory-and-Sales-Management-System Inventory cross-site request forgery	A vulnerability has been found in Mini-Inventory-and-Sales-Management-System and classified as problematic. Affected by this vulnerability is an unknown function of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	NA
		CVE-2022-24235	Snapt Aria 12.8 cross-site request forgery	A vulnerability was found in Snapt Aria 12.8. It has been classified as problematic. This affects an unknown part. The manipulation with an unknown input led to cross-site request forgery. It is possible to initiate	Protected by core rules.	NA



		the attack remotely. There is no exploit available.		
CVE-2021-40662	Chamilo LMS 1.11.14 URL cross-site request forgery	A vulnerability was found in Chamilo LMS 1.11.14. It has been declared as problematic. This vulnerability affects the unknown code of the component. The manipulation with an unknown input led to cross-site request forgery. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	NA
CVE-2022-0616	Amelia Plugin prior 1.0.47 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Amelia Plugin. Affected by this vulnerability is an unknown functionality. The manipulation with an unknown input led to cross-site request forgery. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	NA
CVE-2021-43737	xiaohuanxiong 5.0.17 cross-site request forgery (ID 28)	A vulnerability classified as problematic has been found in xiaohuanxiong 5.0.17. Affected is an unknown function. The manipulation with an unknown input led to cross-site request forgery. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules.	NA
CVE-2022-25576	Anchor CMS 0.12.7 Post anchor/routes/posts.php cross-	A vulnerability classified as problematic has been found in Anchor CMS 0.12.7.	Protected by core rules.	NA



	site request forgery	This affects an unknown part of the file. The manipulation with an unknown input led to cross-site request forgery. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-28143	Proxmox Plugin up to 0.7.0 on Jenkins cross-site request forgery	A vulnerability has been found in Proxmox Plugin up to 0.7.0 and classified as problematic. This vulnerability affects the unknown code. The manipulation led to cross-site request forgery. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	NA
CVE-2022-0770	Translate GTranslate Plugin up to 2.9.8 on WordPress cross-site request forgery	A vulnerability has been found in Translate GTranslate Plugin up to 2.9.8 and classified as problematic. This vulnerability affects the unknown code. The manipulation led to cross-site request forgery. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	NA



3	SQL Injection	CVE-2022-23380	taocms 3.0.2 sql injection	A vulnerability was found in taocms 3.0.2. It has been classified as critical. This affects an unknown function. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2022-23387	taocms up to 3.0.2 Comment Update SQL injection	A vulnerability was found in taocms up to 3.0.2 and classified as critical. This issue affects an unknown functionality. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-40635	OS4Ed openSIS Classic 8.0 ChooseCpSearch.php SQL injection	A vulnerability was found in OS4Ed openSIS Classic 8.0. It has been rated as critical. Affected by this issue is an unknown code of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-40636	OS4Ed openSIS Classic 8.0 CheckDuplicateName.php SQL injection	A vulnerability was found in OS4Ed openSIS Classic 8.0. It has been classified as critical. Affected is some unknown functionality of the file. There is no information about possible countermeasures known. It may be	Protected by core rules.	Detected by the scanner as the SQL Injection attack.



		suggested to replace the affected object with an alternative product.		
CVE-2022-23898	mingSoft MCMS 5.2.5 IContentDao.xml l categoryId SQL injection	A vulnerability, which was classified as critical, has been found in mingSoft MCMS 5.2.5. Affected by this issue is some unknown processing of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2022-25125	mingSoft MCMS 5.2.4 listExcludeApp search.do SQL injection	A vulnerability has been found in mingSoft MCMS 5.2.4 and classified as critical. This vulnerability affects the function of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2022-0507	Artica Pandora FMS up to 759 API SQL injection	A vulnerability was found in Artica Pandora FMS up to 759. It has been classified as problematic. This affects an unknown code of the component API. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2021-32474	Moodle up to 3.5.17/3.8.8/3.9.6/3.10.3 MNet SQL injection	A vulnerability was found in Moodle up to 3.5.17/3.8.8/3.9.6/3.	Protected by core rules.	Detected by the scanner as the SQL



		10.3 (Learning Management Software). It has been rated as critical. This issue affects an unknown part of the component MNet. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		Injection attack.
CVE-2022-25607	FV Flowplayer Video Player Plugin up to 7.5.15.727 on WordPress SQL injection	A vulnerability classified as critical has been found in FV Flowplayer Video Player Plugin up to 7.5.15.727. This affects an unknown part. The manipulation with an unknown input led to SQL injection. This vulnerability is uniquely identified as CVE-2022-25607. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2022-26266	Piwigo 12.2.0 pwg.users.php SQL injection	A vulnerability has been found in Piwigo 12.2.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file pwg.users.php. The manipulation with an unknown input led to SQL injection. This vulnerability is known as CVE-2022-26266. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2021-43735	CmsWing 1.3.7 behavior rule SQL injection (ID 55)	A vulnerability, which was classified as critical, was found in CmsWing 1.3.7. This affects an	Protected by core rules.	Detected by the scanner as the SQL Injection attack.



		unknown part. The manipulation of the argument behavior rule with an unknown input led to SQL injection. This vulnerability is uniquely identified as CVE-2021-43735. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2021-43084	Dreamer CMS 4.0.0 tableName SQL injection	A vulnerability was found in Dreamer CMS 4.0.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument tableName with an unknown input led to SQL injection. The identification of this vulnerability is CVE-2021-43084. The attack may be initiated remotely. There is no exploit available.		Detected by the scanner as the SQL Injection attack.
CVE-2022-26301	yeyinshi TuziCMS 2.0.6 ZhuantiController.class.php SQL injection (ID 11)	A vulnerability was found in yeyinshi TuziCMS 2.0.6. It has been rated as critical. Affected by this issue is some unknown functionality of the file App\Manage\Controller\ZhuantiController.class.php. The manipulation with an unknown input led to SQL injection. This vulnerability is handled as CVE-2022-26301. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2022-26245	Falcon-Plus 0.3 /config/service/host.go grpName SQL	A vulnerability, which was classified as critical, has been found in Falcon-Plus	Protected by core rules.	Detected by the scanner as the SQL



	injection (ID 951)	0.3. This issue affects some unknown processing of the file /config/service/host.go. The manipulation of the argument grpName with an unknown input led to SQL injection. The identification of this vulnerability is CVE-2022-26245. The attack may be initiated remotely. There is no exploit available.		Injection attack.
CVE-2021-26599	ImpressCMS up to 1.4.2 include/findusers.php groups SQL injection	A vulnerability was found in ImpressCMS up to 1.4.2. It has been rated as critical. This issue affects some unknown processing of the file include/findusers.php. The manipulation of the argument groups with an unknown input led to SQL injection. The identification of this vulnerability is CVE-2021-26599. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2022-24956	Shopware up to 4.4.1 Search sort-by SQL injection (SYSS-2022-018)	A vulnerability was found in Shopware up to 4.4.1. It has been rated as critical. Affected by this issue is some unknown functionality of the component Search. The manipulation of the argument sort-by leads to SQL injection. This vulnerability is handled as CVE-2022-24956. The attack may be	Protected by core rules.	Detected by the scanner as the SQL Injection attack.



		launched remotely. There is no exploit available.		
CVE-2020-24769	NexusPHP 1.5 SQL Command takeconfirm.php classes SQL injection	A vulnerability was found in NexusPHP 1.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file takeconfirm.php of the component SQL Command Handler. The manipulation of the argument classes leads to SQL injection. This vulnerability is handled as CVE-2020-24769. The attack may be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		It is recommended to upgrade the affected component.		
CVE-2020-24770	NexusPHP 1.5 modrules.php id SQL injection	A vulnerability classified as critical has been found in NexusPHP 1.5. This affects an unknown part of the file modrules.php. The manipulation of the argument led to SQL injection. This vulnerability is uniquely identified as CVE-2020-24770. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2022-23797	Joomla up to 3.10.6/4.1.0 SQL injection	A vulnerability, which was classified as critical, was found in Joomla up to 3.10.6/4.1.0. This affects an unknown part. The manipulation leads to SQL injection.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.



				<p>This vulnerability is uniquely identified as CVE-2022-23797. It is possible to initiate the attack remotely. There is no exploit available.</p>		
4	Remote Code Execution	CVE-2021-23495	karma up to 6.3.15 Query Parameter return_url redirect	<p>A vulnerability, which was classified as critical, has been found in VMware Spring 9.0. Affected by this issue is some unknown functionality. The manipulation leads to privilege escalation. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.</p>	Protected by custom rules.	NA
5	XML External Entity	CVE-2022-28154	Complexity Scatter Plot Plugin up to 1.1.1 on Jenkins XML Parser XML external entity reference	<p>A vulnerability classified as problematic has been found in Complexity Scatter Plot Plugin up to 1.1.1. Affected is an unknown function of the component XML Parser. The manipulation leads to XML External Entity. This vulnerability is traded as CVE-2022-28154. The attack can only be initiated within the local network. There is no exploit available.</p>	Protected by core rules.	Detected by the scanner as XML External Entity attack.
		CVE-2022-28155	Pipeline Phoenix AutoTest Plugin up to 1.3 on Jenkins XML Parser XML external entity reference	<p>A vulnerability classified as problematic was found in Pipeline Phoenix AutoTest Plugin up to 1.3. Affected by this vulnerability is an unknown functionality of the component XML Parser. The manipulation leads to XML External</p>	Protected by core rules.	Detected by the scanner as XML External Entity attack.



				Entity. This vulnerability is known as CVE-2022-28155. The attack needs to be done within the local network. There is no exploit available.		
		CVE-2022-28140	Flaky Test Handler Plugin up to 1.2.1 on Jenkins XML Parser XML external entity reference	A vulnerability was found in Flaky Test Handler Plugin up to 1.2.1. It has been rated as problematic. This issue affects some unknown processing of the component XML Parser. The manipulation leads to XML External Entity. The identification of this vulnerability is CVE-2022-28140. The attack can only be done within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as XML External Entity attack.
6	Local File Inclusion	CVE-2022-23377	Archeevo up to 4.x file file inclusion	A vulnerability was found in Archeevo up to 4.x and classified as problematic. Affected by this issue is some unknown processing. Upgrading to version 5.0 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
		CVE-2021-42767	Neo4j Graph Database up to 4.3.6 Apoc Plugin pathname traversal	A vulnerability was found in Neo4j Graph Database up to 4.3.6. It has been classified as problematic. Affected is an unknown code block of the component Apoc Plugin. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.



CVE-2022-26315	qrcp up to 0.8.4 File Name path traversal	A vulnerability, which was classified as critical, was found in qrcp up to 0.8.4. Affected is an unknown function of the component File Name Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2021-3762	Clair ClairCore Engine path traversal	A vulnerability, which was classified as critical, has been found in Clair (unknown version). This issue affects an unknown code of the component ClairCore Engine. Applying the patch 691f2023a1720a057 9e688b69a2f4bfe1f4 b7821 is able to eliminate this problem. The bugfix is ready for download at github.com.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-26484	Veritas InfoScale Operations Manager up to 7.4.2/8.0.0 Configuration File pathname traversal	A vulnerability was found in Veritas InfoScale Operations Manager up to 7.4.2/8.0.0. It has been classified as problematic. This affects some unknown processing of the file admin/cgi- bin/rulemgr.pl/getfil e/ of the component Configuration File Handler. Applying the patch 7.4.2 Patch 600/8.0.0 Patch 100 is able to eliminate this problem.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-24716	Icinga Web up to 2.9.5 Configuration File path traversal	A vulnerability classified as critical has been found in Icinga Web up to 2.9.5. Affected is an	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.



		unknown functionality of the component Configuration File Handler. Upgrading to version 2.9.6 or 2.10 eliminates this vulnerability. Applying the patch 9931ed799650f5b8d5e1dc58ea3415a4cdc5773d is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.		
CVE-2022-24715	Icinga Web up to 2.8.5/2.9.5/2.9 SSH Resource File path traversal	A vulnerability was found in Icinga Web up to 2.8.5/2.9.5/2.9. It has been declared as critical. This vulnerability affects some unknown processing of the component SSH Resource File Handler. Upgrading to version 2.8.6, 2.9.6 or 2.10 eliminates this vulnerability. Applying the patch a06d915467ca943a4b406eb9587764b8ec34cafb is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-26652	NATS nats-server up to 2.7.3 ZIP Archive pathname traversal	A vulnerability was found in NATS nats-server up to 2.7.3. It has been classified as critical. This affects an unknown functionality of the	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.



		component ZIP Archive Handler. Upgrading to version 2.7.4 eliminates this vulnerability.		
CVE-2022-26276	OneNav 0.9.14 index.php path traversal	A vulnerability, which was classified as critical, has been found in OneNav 0.9.14. This issue affects an unknown functionality of the file index.php. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-25216	DVDFab Player 12 HTTP GET Request /download/ path traversal	A vulnerability was found in DVDFab Player 12 and classified as critical. Affected by this issue is an unknown part of the file /download/ of the component HTTP GET Request Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-26960	std42 elFinder up to 2.1.60 connector.minimal.php path traversal	A vulnerability was found in std42 elFinder up to 2.1.60. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file connector.minimal.php. The manipulation with an unknown input led to directory traversal. This vulnerability is known as CVE-2022-26960. The attack	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.



		can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2022-23347	Bigantsoft BigAnt Server 5.6.06 pathname traversal	A vulnerability was found in Bigantsoft BigAnt Server 5.6.06. It has been classified as critical. This affects an unknown part. The manipulation with an unknown input led to directory traversal. This vulnerability is uniquely identified as CVE-2022-23347. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-25266	Passwork On-Premises Edition prior 4.6.13 downloadExport File pathname traversal	A vulnerability was found in Passwork On-Premise Edition. It has been rated as problematic. This issue affects some unknown processing of the file migration/download ExportFile. The manipulation with an unknown input led to directory traversal. The identification of this vulnerability is CVE-2022-25266. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2022-27906	Mendelson OFTP2 prior 1.1b43 Upload Directory pathname traversal	A vulnerability classified as critical was found in Mendelson OFTP2. Affected by this vulnerability is an unknown functionality of the component Upload	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.



		Directory Handler. The manipulation with an unknown input led to directory traversal. This vulnerability is known as CVE-2022-27906. The attack can only be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-26271	74cmsSE 3.4.1 Download.php URL path traversal	A vulnerability has been found in 74cmsSE 3.4.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file <code>\index\controller\Download.php</code> . The manipulation of the argument URL with an unknown input led to directory traversal. This vulnerability is known as CVE-2022-26271. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.
CVE-2021-26601	ImpressCMS up to 1.4.2 image-edit.php image_temp pathname traversal	A vulnerability classified as critical has been found in ImpressCMS up to 1.4.2. Affected is an unknown function of the file <code>libraries/image-editor/image-edit.php</code> . The manipulation of the argument <code>image_temp</code> with an unknown input led to directory traversal. This vulnerability is traded as CVE-2021-26601. The attack can only be initiated	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.



			within the local network. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2021-44124	HiByMusic HiBy OS up to 1.5/1.6 HTTP Server pathname traversal	A vulnerability classified as critical was found in HiBy Music HiByOS up to 1.5/1.6. This vulnerability affects unknown code of the component HTTP Server. The manipulation led to directory traversal. This vulnerability was named CVE-2021-44124. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.	
CVE-2022-28157	Pipeline Phoenix AutoTest Plugin up to 1.3 on Jenkins FTP path traversal	A vulnerability has been found in Pipeline Phoenix AutoTest Plugin up to 1.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the component FTP Handler. The manipulation led to directory traversal. This vulnerability is known as CVE-2022-28157. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.	
CVE-2022-23793	Joomla up to 3.10.6/4.1.0 tar path traversal (ID 166546)	A vulnerability classified as critical was found in Joomla up to 3.10.6/4.1.0. Affected by this vulnerability is an unknown functionality of the component tar Handler. The manipulation led to directory traversal. This vulnerability is known as CVE-2022-	Protected by core rules.	Detected by the scanner as Local File Inclusion attack.	



				23793. Access to the local network is required for this attack to succeed. There is no exploit available.		
7	Cross-Site Scripting	CVE-2022-25022	Htmlly 2.8.1 Blog Post content cross-site scripting	A vulnerability was found in Htmlly 2.8.1 and classified as problematic. This issue affects an unknown code of the component Blog Post Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-25015	Ice Hrm 30.0.0.OS First Name cross-site scripting	A vulnerability, which was classified as problematic, has been found in Ice Hrm 30.0.0.OS. Affected by this issue is an unknown functionality. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2022-0906	Microweber up to 1.1.11 File Upload cross-site scripting	A vulnerability, which was classified as problematic, has been found in Microweber up to 1.1.11. Affected by this issue is an unknown code of the component File Upload Handler. Upgrading to version 1.1.12 eliminates this vulnerability. Applying the patch d9bae9df873c2d2a13a2eb08d512019d49ebca68 is able to eliminate this problem. The bugfix	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.



		is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.		
CVE-2022-0928	microweber up to 1.2.11 cross-site scripting	A vulnerability was found in microweber up to 1.2.11. It has been classified as problematic. This affects an unknown part. Upgrading to version 1.2.12 eliminates this vulnerability. Applying the patch fc9137c031f7edec5f50d73b300919fb519c924a is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-24177	Ex libris ALEPH 500 18.1/20 cgi-bin/ej.cgi cross-site scripting	A vulnerability classified as problematic has been found in Ex libris ALEPH 500 18.1/20. This affects an unknown function of the file cgi-bin/ej.cgi. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-0930	microweber up to 1.2.11 Upload Filter cross-site scripting	A vulnerability was found in microweber up to 1.2.11. It has been declared as problematic. This vulnerability affects some unknown processing of the component Upload Filter Handler.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.



		Upgrading to version 1.2.12 eliminates this vulnerability. Applying the patch 33eb4cc0f80c1f86388c1862a8aee1061fa5d72e is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.		
CVE-2022-0929	microweber up to 1.2.10 dynamic_text Module cross-site scripting	A vulnerability was found in microweber up to 1.2.10. It has been classified as problematic. This affects an unknown code block of the component dynamic_text Module. Upgrading to version 1.2.11 eliminates this vulnerability. Applying the patch de6d17b52d261902653fbdd2ecefcaac82e54256 is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-23150	CVE-2021-23150 Accelerated Mobile Pages Plugin up to 1.0.77.31 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Accelerated Mobile Pages Plugin up to 1.0.77.31. This affects an unknown part. The manipulation with an unknown input led to crosssite scripting. This vulnerability is uniquely identified	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.



		as CVE-2021-23150. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2022-25604	Price Table Plugin up to 0.2.2 on WordPress cross-site scripting	A vulnerability has been found in Price Table Plugin up to 0.2.2 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation with an unknown input led to cross-site scripting. This vulnerability is known as CVE-2022-25604. The attack can be launched remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-23209	Accelerated Mobile Pages Plugin on WordPress cross-site scripting	A vulnerability classified as problematic was found in Accelerated Mobile Pages Plugin. This vulnerability affects unknown code. The manipulation with an unknown input led to cross-site scripting. This vulnerability was named CVE-2021-23209. The attack can be initiated remotely. There is no exploit available.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-0423	3D FlipBook Plugin up to 1.12.0 on WordPress Setting cross-site scripting	A vulnerability was found in 3D FlipBook Plugin up to 1.12.0. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation with an unknown input led to cross-site scripting. This vulnerability is traded as CVE-2022-0423. It is possible	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.



		to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2021-25019	Squirrly SEO Plugin up to 11.1.11 on WordPress Admin Page type cross-site scripting	A vulnerability was found in Squirrly SEO Plugin up to 11.1.11. It has been declared as problematic. This vulnerability affects unknown code of the component Admin Page. The manipulation of the argument type with an unknown input led to cross-site scripting. This vulnerability was named CVE-2021-25019. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-0600	Conference Scheduler Plugin up to 2.4.2 on WordPress Admin Page tab cross-site scripting	A vulnerability was found in Conference Scheduler Plugin up to 2.4.2. It has been classified as problematic. This affects an unknown part of the component Admin Page. The manipulation of the argument tab led to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-0600. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2022-0619	Database Peek Plugin up to 1.2 on WordPress Admin Page match cross-site scripting	A vulnerability was found in Database Peek Plugin up to 1.2. It has been declared as problematic. This	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.



				<p>vulnerability affects the unknown code of the component Admin Page. The manipulation of the argument match leads to cross-site scripting. This vulnerability was named CVE-2022-0619. The attack can be initiated remotely. There is no exploit available.</p>
CVE-2022-22963	Spring Cloud Function injection	A vulnerability was found in Spring Cloud Function and classified as critical. Affected by this issue is the unknown functionality. The manipulation leads to privilege escalation. This vulnerability is handled as CVE-2022-22963. The attack may be launched remotely. Furthermore, there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by custom rules.	Detected by the scanner as the Cross-Site Scripting attack.
