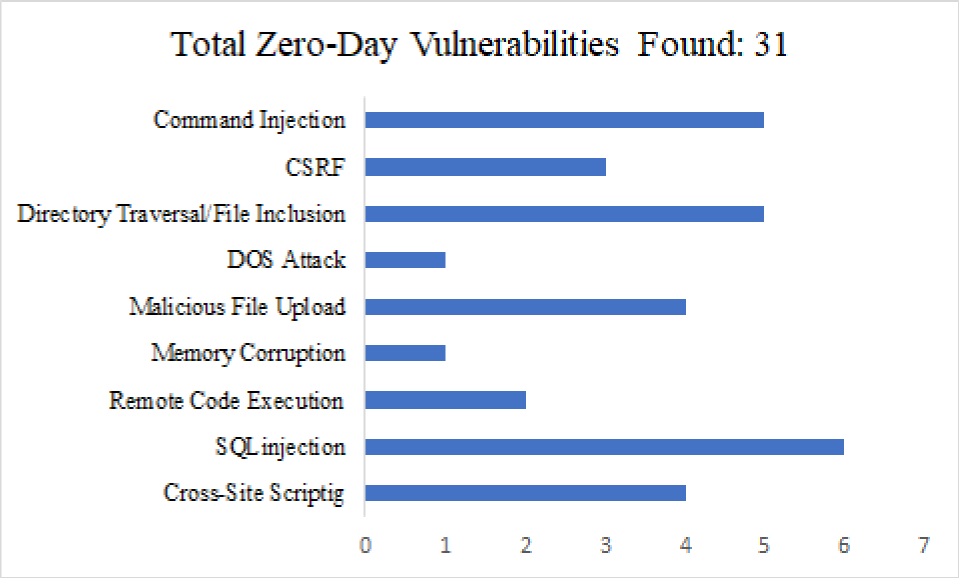
Monthly Zero-Day Vulnerability Coverage Bulletin

August 2021



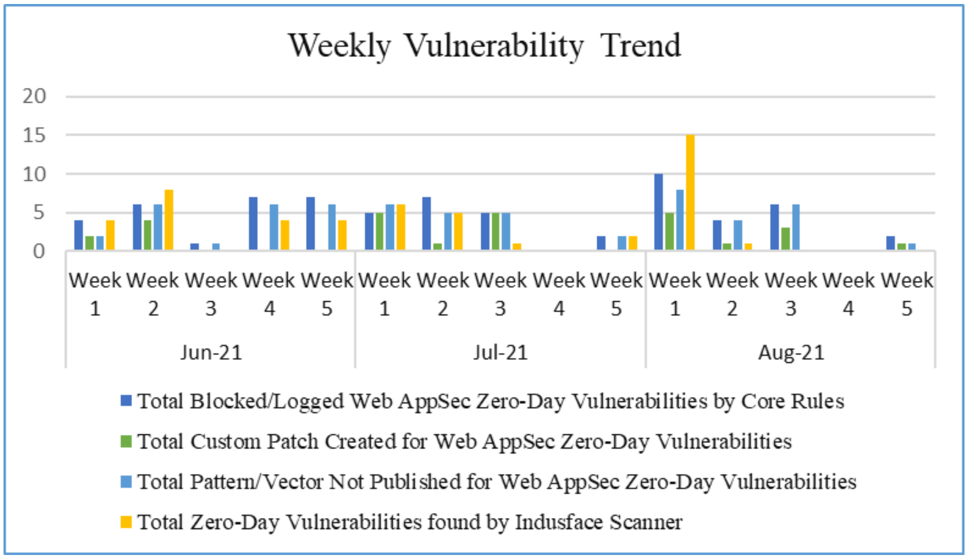
Zero-Day vulnerabilities protected through core rules	22
Zero-Day vulnerabilities protected through custom rules	9 *
Zero-Day vulnerabilities for which protection cannot be determined	0 **
Zero-Day vulnerabilities found by Indusface WAS	20

* 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:

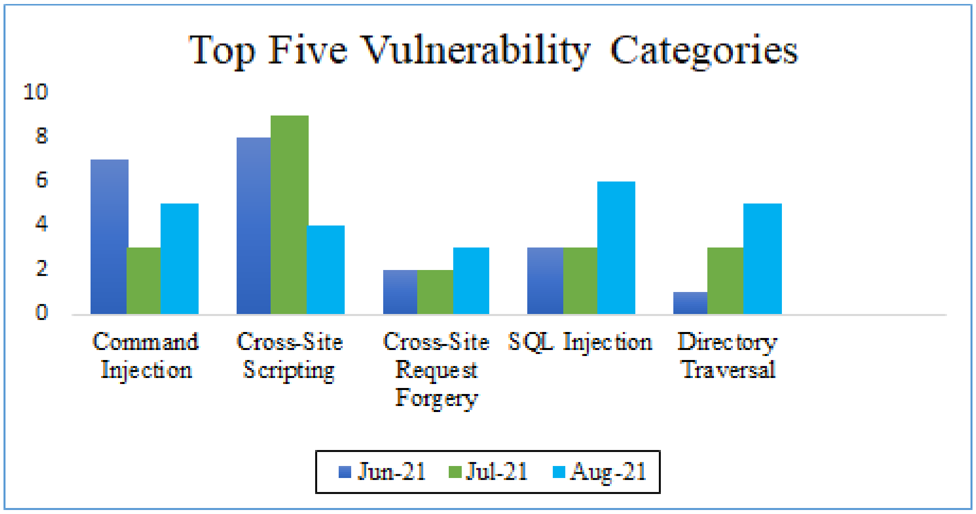
The weekly trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



71% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

29% of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

65% 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-2021-36024	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 Data Collection Endpoint os command injection	A vulnerability was found in Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1. It has been classified as critical. This affects an unknown code block of the component Data Collection Endpoint. The manipulation with an unknown input led to a privileged escalation vulnerability. CWE is classifying the issue as CWE-78. This is going to have an impact on confidentiality, integrity, and availability.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		CVE 2020-5902	Critical Vulnerability in F5 BIG-IP Traffic Management User Interface (TMUI) Actively Exploited	CVE-2020-5902 is a critical vulnerability in the BIG-IP Traffic Management User Interface (TMUI) also known as the Configuration Utility. The vulnerability received a CVSSv3 rating of 10.0, the highest possible score. The vulnerability is exploitable when network access to the TMUI is exposed via the BIG-IP management port or Self IPs. Successful exploitation of this flaw would grant an attacker a variety of	Protected by core rules.	Detected by the scanner as the Command Injection attack.

			privileges, including the ability to execute arbitrary system commands or Java code, create or delete files, as well as disabled services on the vulnerable host. The advisory states that the vulnerability could also “result in complete system compromise.”		
	CVE-2019-11580	Atlassian Crowd/Crowd Data Center up to 3.0.4/3.1.5/3.2.7/3.3.4/3.4.3 pdkinstall input validation	A vulnerability has been found in Atlassian Crowd and Crowd Data Center up to 3.0.4/3.1.5/3.2.7/3.3.4/3.4.3 and classified as critical. Affected by this vulnerability is an unknown code of the component pdkinstall. The manipulation with an unknown input led to a privileged escalation vulnerability. The CWE definition for the vulnerability is CWE-20. As an impact it is known to affect confidentiality, integrity, and availability.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
	CVE-2019-0604	Microsoft SharePoint Server Application Package input validation	A vulnerability was found in Microsoft SharePoint Server (Groupware Software). It has been rated as critical. Affected by this issue is an unknown code of the component Application Package Handler. The	Protected by core rules.	Detected by the scanner as the Command Injection attack.

			manipulation with an unknown input led to a privileged escalation vulnerability. Using CWE to declare the problem leads to CWE-20. Impacted is confidentiality, integrity, and availability. The weakness was presented 02/12/2019 as confirmed security update guide (Website). The advisory is available at portal.msrc.microsoft.com. The public release was coordinated in cooperation with the vendor. This vulnerability is handled as CVE-2019-0604. Exploration is known to be easy. The attack may be launched remotely. Simple authentication is needed for exploitation. Technical details are unknown, but public exploit is available.		
	CVE-2021-36800	Akaunting up to 2.1.12 Money.php code injection	A vulnerability was found in Akaunting up to 2.1.12 and classified as critical. Affected by this issue is an unknown code of the file Money.php. The manipulation of the argument items [0] [price] with an	Protected by core rules.	Detected by the scanner as the Command Injection attack.

				unknown input led to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-94. Impacted is confidentiality, integrity, and availability.		
2	Cross-Site Request Forgery	CVE-2021-34632	SEO Backlinks Plugin up to 4.0.1 on WordPress ~/seo-backlinks.php loc_config cross-site request forgery	A vulnerability has been found in WordPress and classified as problematic. This vulnerability affects the function. There is no information about countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by custom rules.	NA
		CVE-2021-34628	Admin Custom Login Plugin up to 3.2.7 on WordPress Login-form-background.php cross-site request forgery	A vulnerability, which was classified as problematic, was found in Admin Custom Login Plugin up to 3.2.7. This affects an unknown code block of the file. There is no information about countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by custom rules.	NA
		CVE-2021-34633	Youtube Feeder Plugin up to 2.0.1 on WordPress ~/youtube-feeder.php printAdminPage cross-site request forgery	A vulnerability classified as problematic has been found in Youtube Feeder Plugin up to 2.0.1. Affected is the function. Applying a patch is able to	Protected by custom rules.	NA

				eliminate this problem.		
3	Directory Traversal/File Inclusion	CVE-2021-36031	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 Parameter theme[preview_image] path traversal	A vulnerability classified as critical was found in Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1. Affected by this vulnerability is some unknown functionality of the component Parameter Handler. The manipulation of the argument theme[preview_image] with an unknown input led to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability.	Protected by core rules.	Detected by the scanner as the Directory Traversal attack.
		CVE-2021-32804	node-tar up to 3.2.1/3.3.1/4.4.13/5.0.5/6.1.0 on npm File Creation Creation/Overwrite path traversal	A vulnerability, which was classified as problematic, was found innode-tar up to 3.2.1/3.3.1/4.4.13/5.0.5/6.1.0. This affects some unknown functionality of the file. Upgrading to version 3.2.2, 3.3.2, 4.4.14, 5.0.6 or 6.1.1 eliminates this vulnerability. Applying a patch is able to eliminate this problem.	Protected by core rules	Detected by the scanner as the Directory Traversal attack.
		CVE-2020-19304	MetInfo 7.0.0 Directory index.php pathname traversal	A vulnerability was found inMetInfo 7.0.0. It has been classified as problematic. This	Protected by core rules	Detected by the scanner as the Directory Traversal attack.

			affects some unknown processing of the file. There is no information about countermeasures known. It may be suggested to replace the affected object with an alternative product.		
	CVE-2019-19781	Citrix Application Delivery Controller/Gateway 10.5/11.1/12.0/12.1/13.0 directory traversal	A vulnerability was found in Citrix Application Delivery Controller and Gateway 10.5/11.1/12.0/12.1/13.0 (Connectivity Software). It has been classified as very critical. Affected is some unknown processing. The manipulation with an unknown input led to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality, integrity, and availability.	Protected by core rules	Detected by the scanner as the Directory Traversal attack.
	CVE 2018-13379	Fortinet FortiOS up to 6.0.4 SSL VPN Web Portal path traversal	CVE-2018-13379 is a path traversal vulnerability in Fortinet’s FortiGate SSL VPN. An unauthenticated, remote attacker could exploit this vulnerability by sending a specially crafted request containing a path traversal sequence to a vulnerable Fortigate SSL VPN endpoint in order to	Protected by core rules	Detected by the scanner as the Directory Traversal attack.

	read arbitrary files from the device. This vulnerability is a pre-authentication flaw, which means an attacker does not need to be authenticated to the vulnerable device in order to exploit it. Successful exploitation would allow the attacker to read the contents of the “sslvpn_websesion” session file that contains both usernames and plaintext passwords.	

4	DOS Attack	CVE-2021-36802	Akaunting up to 2.1.12 HTTP POST Request locale denial of service	A vulnerability has been found in Akaunting up to 2.1.12 and classified as problematic. This vulnerability affects an unknown part of the component HTTP POST Request Handler. The manipulation of the argument locale with an unknown input led to denial-of-service vulnerability. The CWE definition for the vulnerability is CWE-404. As an impact it is known to affect availability.	Protected by custom rules	NA
5	Malicious File Upload	CVE-2021-36034	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 unrestricted upload	A vulnerability, which was classified as critical, was found in Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1. This affects an unknown code. The manipulation with an unknown input led to a privileged escalation vulnerability. CWE is classifying the issue as CWE-434. This is going to have an impact on confidentiality, integrity, and availability.	Protected by custom rules.	NA
		CVE-2021-36040	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 File Extension unrestricted upload	A vulnerability has been found in Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 and classified as critical. This vulnerability affects an unknown code block of the component File	Protected by core rules.	Detected by the scanner as the Malicious File Upload attack.

		Extension Handler. The manipulation with an unknown input led to a privileged escalation vulnerability. The CWE definition for the vulnerability is CWE-434. As an impact it is known to affect confidentiality, integrity, and availability.		
CVE-2021-36042	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 File Upload unrestricted upload	A vulnerability was found in Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1. It has been classified as critical. Affected is an unknown function of the component File Upload Handler. The manipulation with an unknown input led to a privileged escalation vulnerability. CWE is classifying the issue as CWE-434. This is going to have an impact on confidentiality, integrity, and availability.	Protected by custom rules.	NA
CVE-2021-34639	Download Manager up to 3.1.24 on WordPress unrestricted upload	A vulnerability was found in Download Manager up to 3.1.24. It has been declared as critical. This vulnerability 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 Malicious File Upload attack.

6	Memory corruption	CVE-2017-11882	Microsoft Office memory corruption	A vulnerability, which was classified as critical, has been found in Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016 (Office Suite Software). Affected by this issue is some unknown processing. The manipulation with an unknown input led to memory corruption vulnerability. Using CWE to declare the problem leads to CWE-119. Impacted is confidentiality, integrity, and availability. The bug was discovered 11/14/2017. The weakness was presented 11/14/2017 with Embedi as KB4011276 as confirmed security update guide (Website). The advisory is shared for download at portal.msrc.microsoft.com. This vulnerability has been handled as CVE-2017-11882 since 07/31/2017. The attack may be launched remotely. No form of authentication is required for exploitation. Successful exploitation requires user interaction by	Protected by custom rules.	NA

				the victim. Technical details are unknown, but public exploit is available.		
7	Remote Code Execution (RCE)	CVE-2021-34473	Drupal up to 7.57/8.3.8/8.4.5/8.5.0 input validation	A vulnerability was found in Drupal up to 7.57/8.3.8/8.4.5/8.5.0 (Content Management System). It has been classified as critical. This affects an unknown code block. The manipulation with an unknown input led to a privileged escalation vulnerability. CWE is classifying the issue as CWE-20. This is going to have an impact on confidentiality, integrity, and availability. The bug was discovered 03/28/2018. The weakness was disclosed 03/29/2018 by Matt (Website). The advisory is shared at lists.debian.org. This vulnerability is uniquely identified as CVE-2018-7600 since 03/01/2018. The exploitability is said to be easy. It is possible to initiate the attack remotely.	Protected by custom rules.	NA
		CVE-2021-34523	Telerik UI - Remote Code Execution via Insecure Deserialization	The vulnerability in Telerik relies on type of the object in rauPostData, allowing them to control the object's behavior while it is being deserialized. A remote code	Protected by custom rules.	NA

				execution (RCE) gadget's properties allow it to perform operations that facilitate executing arbitrary code.		
8	SQL Injection	CVE-2021-24463	Responsive Slider and Carousel Plugin up to 2.4.x Admin Dashboard get_sliders orderby sql injection	A vulnerability has been found in Responsive Slider and Carousel Plugin up to 2.4.x and classified as critical. This vulnerability affects the function of the component. Upgrading to version 2.5.0 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-36455	Navigate CMS 2.9 comments.php quicksearch sql injection	A vulnerability was found in Navigate CMS 2.9 and classified as critical. This issue affects an unknown function of the file. Upgrading to version 2.9.4 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		NA	jeecg-boot CMS 2.3 loadtreedata sql injection	A vulnerability classified as critical has been found injeecg-boot CMS. Affected is an unknown part of the file. There is no information about 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-2020-20981	Metinfo 7.0 sql injection [CVE-2020-20981]	A vulnerability was found in Metinfo. It has been rated as critical. Affected by this issue is an unknown code of the file. There is no information about countermeasures	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

		known. It may be suggested to replace the affected object with an alternative product.		
CVE-2021-31867	Pimcore Customer Data Framework up to 3.0.0 SegmentAssignmentController.php id sql injection	A vulnerability has been found in Pimcore Customer Data Framework up to 3.0.0 and classified as critical. Affected by this vulnerability is an unknown part of the file SegmentAssignmentController.php. The manipulation of the argument id with an unknown input led to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
CVE-2021-31869	Pimcore AdminBundle v6.8.0	A vulnerability was found in Pimcore AdminBundle up to 6.8.0. It has been rated as critical. This issue affects an unknown code block. The manipulation of the argument specificID with an unknown input led to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

				confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.		
9	Cross-Site Scripting	CVE-2021-24455	eLearning and online course solution Plugin up to 1.9.1 on WordPress cross site scripting	The Tutor LMS &#8211; eLearning and online course solution WordPress plugin before 1.9.2 did not escape the Summary field of Announcements (when outputting it in an attribute), which can be created by users as low as Tutor Instructor. This led to a Stored Cross-Site Scripting issue, which is triggered when viewing the Announcements list, and could result in privilege escalation when viewed by an admin.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-3539	EspoCRM up to 6.1.6 Avatar Image cross site scripting	A vulnerability was found in EspoCRM up to 6.1.6. It has been declared as problematic. Affected by this vulnerability is some unknown processing of the component Avatar Image Handler. The manipulation with an unknown input led to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-79. As an impact it is known to	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

		affect integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.		
CVE-2021-36803	Akaunting up to 2.1.12 Avatar Image cross site scripting	A vulnerability was found in Akaunting up to 2.1.12. It has been rated as problematic. Affected by this issue is an unknown function of the component Avatar Image Handler. The manipulation with an unknown input led to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-36805	Akaunting up to 2.1.12 Sales Invoice cross site scripting	A vulnerability classified as problematic has been found in Akaunting up to 2.1.12. This affects an unknown functionality of the component Sales Invoice Handler. The manipulation with an	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

unknown input led to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.