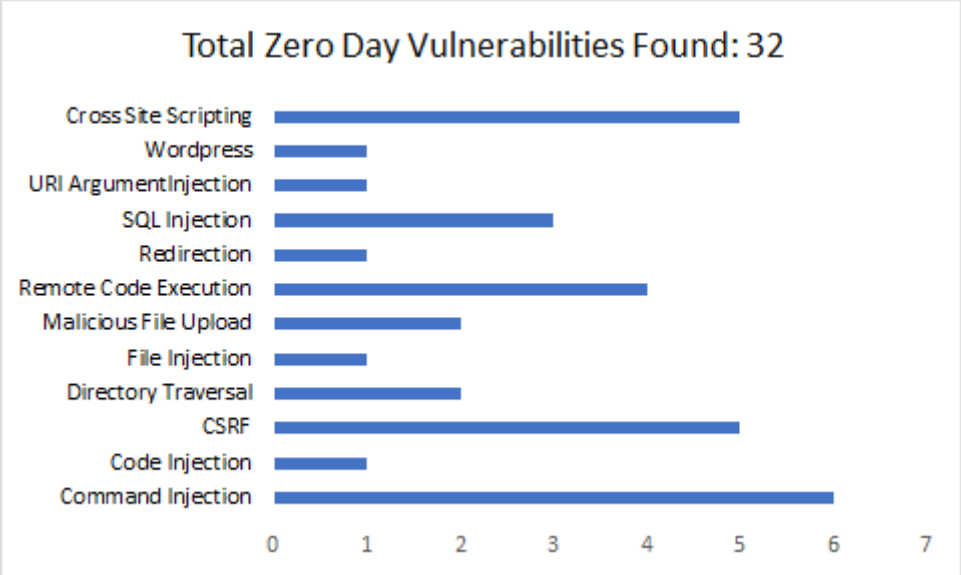
Weekly Zero-Day Vulnerability Coverage Bulletin

September 2021



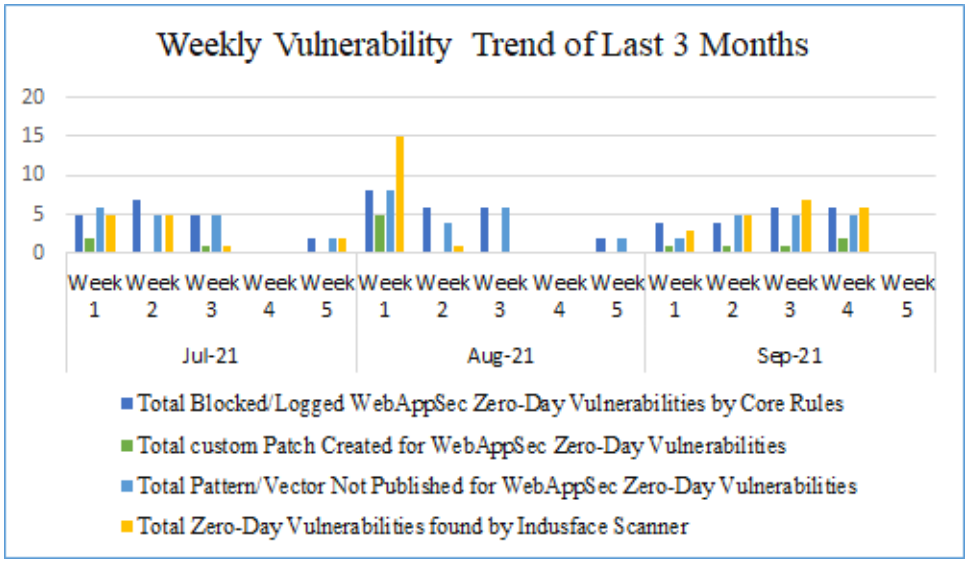
Zero-Day Vulnerabilities Protected through Core Rules	20
Zero-Day Vulnerabilities Protected through Custom Rules	10 *
Zero-Day Vulnerabilities for which protection cannot be determined	2 **
Zero-Day Vulnerabilities found by Indusface WAS	18

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

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

Vulnerability Trend:

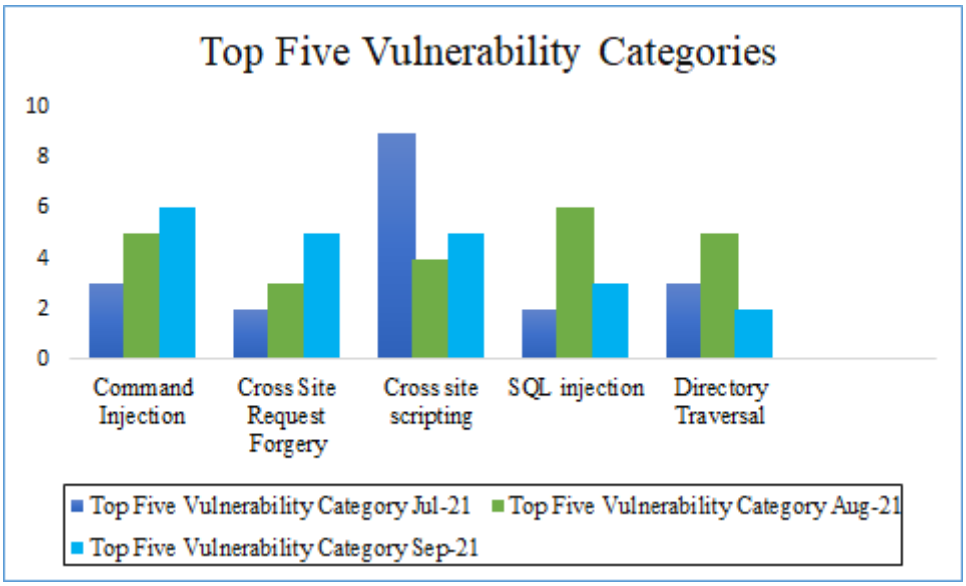
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



63% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

31% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

56% Of Zero-Day Vulnerabilities were reported by Indusface Scanner in 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 around 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-2021-37346	Nagios XI WatchGuard Wizard os command injection	Nagios XI WatchGuard Wizard before version 1.4.8 is vulnerable to remote code execution through Improper neutralization of special elements used in an OS command (OS Command injection).	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2021-37344	Nagios XI Switch Wizard os command injection	Nagios XI Switch Wizard before version 2.5.7 is vulnerable to remote code execution through improper neutralization of special elements used in an OS command (OS Command injection).	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2021-3723	Command Injection Vulnerability in Legacy IBM System x IMM	A command injection vulnerability was reported in the Integrated Management Module (IMM) of legacy IBM System x 3550 M3 and IBM System x 3650 M3 servers that could allow the execution of operating system commands over an authenticated SSH or Telnet session.	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2021-22868	GitHub Enterprise Server up to 2.22.21/3.0.15/3.1.8 Pages Site command injection	A vulnerability, which was classified as problematic, has been found in GitHub Enterprise Server. This issue affects an unknown	Protected by core rules.	Detected by scanner as Command Injection attack.

			code of the component. Upgrading to version 2.22.22, 3.0.16 or 3.1.8 eliminates this vulnerability.		
	CVE-2021-3781	Ghostscript vulnerability CVE-2021-3781	The file access protection built into Ghostscript proved insufficient for the "%pipe%" PostScript device, when combined with Ghostscript's requirement to be able to create and control temporary files in the conventional temporary file directories (for example, "/tmp" or "/temp). This exploit is restricted to Unix-like systems (i.e., it doesn't affect Windows). The most severe claimed results are only feasible if the exploit is run as a "high privilege" user (root/superuser level) \u2013 a practice we would discourage under any circumstances.	Protected by core rules.	Detected by scanner as Command Injection attack.
	CVE-2021-34352	QNAP QVR os command injection	A vulnerability was found in QNAP QVR. It has been rated as critical. This issue affects an unknown functionality. The manipulation with an unknown input leads to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-78. Impacted is confidentiality, integrity, and availability.	Protected by core rules.	Detected by scanner as Command Injection attack.

	The weakness was presented 10/01/2021 as qsa-21-38. The advisory is shared at qnap.com. The identification of this vulnerability is CVE-2021-34352 since 06/08/2021. The exploitation is known to be easy. The attack may be initiated remotely. Additional levels of successful authentication are necessary for exploitation.

2	Code Injection	CVE-2021-26084	Atlassian Confluence Server/Confluence Data Center up to 6.13.22/7.4.10/7.11.5/7.12.4 Webwork OGNL injection	A vulnerability was found in Atlassian Confluence Server and Confluence Data Center up to 6.13.22/7.4.10/7.11.5/7.12.4 and classified as critical. Affected by this issue is an unknown code of the component Webwork OGNL Handler. The manipulation with an unknown input leads to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-74. Impacted is confidentiality, integrity, and availability.	Protected by core rules.	Detected by scanner as Code Injection attack.
3	Cross Site Request Forgery	CVE-2021-38342	Nested Pages Plugin up to 3.1.15 on WordPress Ownership npBulkAction/npBulkEdit/admin_post cross-site request forgery	A vulnerability, which was classified as problematic, was found in Nested Pages Plugin up to 3.1.15 on WordPress (WordPress Plugin). This affects the function npBulkAction/npBulkEdit/admin_post of the component Ownership Handler. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application.	Protected by custom rules.	NA

	CVE-2021-38705	ClinicCases 7.3.3 cross-site request forgery [CVE-2021-38705]	A vulnerability classified as problematic has been found in ClinicCases. This 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 custom rules.	NA
	CVE-2020-20671	Kitesky KiteCMS 1.1 cross-site request forgery [CVE-2020-20671]	A vulnerability was found in Kitesky KiteCMS 1.1. It has been declared as problematic. Affected by this vulnerability is an unknown part. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by custom rules.	NA
	CVE-2020-13673	Drupal core - Moderately critical - Cross Site Request Forgery - SA-CORE-2021-006	The Drupal core Media module allows embedding internal and external media in content fields. In certain circumstances, the filter could allow an unprivileged user to inject HTML into a page when it is accessed by a trusted user with permission to embed media. In some cases, this could lead to cross-site scripting.	Protected by custom rules.	NA
	CVE-2020-13674	Drupal core - Moderately critical - Cross Site Request	The QuickEdit module does not properly validate access to routes,	Protected by custom rules.	NA

			Forgery - SA-CORE-2021-007	which could allow cross-site request forgery under some circumstances and lead to possible data integrity issues. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed. Removing the "access in-place editing" permission from untrusted users will not fully mitigate the vulnerability.		
4	Directory Traversal/File Inclusion	CVE-2021-36233	MIK.starlight 7.9.5.24363 AdminGetFirstFileContentByFilePath path traversal	A vulnerability was found in MIK.starlight 7.9.5.24363. It has been rated as problematic. Affected by this issue is the function: AdminGetFirstFileContentByFilePath. 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 scanner as Directory Traversal attack.
		CVE-2021-37343	Nagios XI AutoDiscovery path traversal	A path traversal vulnerability exists in Nagios XI below version 5.8.5 AutoDiscovery component and could lead to post-authenticated RCE under the security context of the user running Nagios.	Protected by core rules.	Detected by scanner as Directory Traversal attack.

5	File Injection	CVE-2021-37348	Nagios XI index.php file inclusion	Nagios XI before version 5.8.5 is vulnerable to local file inclusion through improper limitation of a pathname in index.php.	Protected by core rules.	Detected by scanner as File Injection attack.
6	Malicious File Upload	CVE-2021-22005	Critical File Upload Vulnerability in VMware vCenter Server	A vulnerability, which was classified as critical, has been found in VMware vCenter Server (Server Management Software) (unknown version). This issue affects some unknown processing of the component Analytics Service. The manipulation with an unknown input leads to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-434. Impacted is confidentiality, integrity, and availability.	Protected by core rules.	Detected by scanner as Malicious File upload attack.
		CVE-2020-13675	Drupal core - Moderately critical - Access bypass - SA-CORE-2021-008	Drupal's JSON:API and REST/File modules allow file uploads through their HTTP APIs. The modules do not correctly run all file validation, which causes an access bypass vulnerability. An attacker might be able to upload files that bypass the file validation process implemented by modules on the site.	Protected by core rules.	Detected by scanner as Malicious File upload attack.

7	Remote Code Execution	CVE-2021-33766	Microsoft Exchange Server 2013 CU23/2016 CU20/2016 CU21/2019 CU9/2019 CU10 information disclosure	A vulnerability has been found in Microsoft Exchange Server 2013 CU23/2016 CU20/2016 CU21/2019 CU9/2019 CU10 (Groupware Software) and classified as problematic. This vulnerability affects an unknown function. The manipulation with an unknown input leads to a information disclosure vulnerability. The CWE definition for the vulnerability is CWE-200. As an impact it is known to affect confidentiality.	Protected by custom rules.	NA
		CVE-2021-31166	Microsoft Windows 10 20H2/10 2004/Server 20H2/Server 2004 HTTP Protocol Stack Remote Code Execution	A vulnerability has been found in Microsoft Windows 10 20H2/10 2004/Server 20H2/Server 2004 (Operating System) and classified as very critical. Affected by this vulnerability is an unknown code block of the component HTTP Protocol Stack. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published 05/11/2021 as confirmed security guidance (Website). The advisory is shared at	Protected by custom rules.	NA

			portal.msrc.microsoft.com. This vulnerability is known as CVE-2021-31166 since 04/14/2021. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details are unknown but a public exploit is available.		
	CVE-2021-40444	Microsoft Windows MSHTML Remote Code Execution [CVE-2021-40444]	A vulnerability was found in Microsoft Windows. It has been declared as critical. This vulnerability affects an unknown part of the component. It is possible to mitigate the problem by applying the configuration setting. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Protected by custom rules.	NA
	CVE-2021-34407	Zoom RCE from Pwn2Own 2021	Research queue	Research queue	NA

8	Redirection	CVE-2021-37352	Nagios XI redirect	An open redirect vulnerability exists in Nagios XI before version 5.8.5 that could lead to spoofing. To exploit the vulnerability, an attacker could send a link that has a specially crafted URL, and convince the user to click the link.	Research queue	NA
9	SQL Injection	CVE-2021-24391	Cashtomer Plugin up to 1.0.0 on WordPress GET Parameter editid sql injection	A vulnerability was found in Cashtomer Plugin up to 1.0.0 on WordPress and classified as critical. Affected by this issue is an unknown code block 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.	Detected by scanner as SQL Injection attack.
		CVE-2021-37350	Nagios XI Bulk Modifications Tool sql injection	Nagios XI before version 5.8.5 is vulnerable to SQL injection vulnerability in the Bulk Modifications Tool due to improper input sanitization.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2021-38833	PHPGurukul Apartment Visitors Management System 1.0 sql injection	A vulnerability, which was classified as critical, has been found in PHPGurukul Apartment Visitors Management System 1.0. This issue affects some unknown functionality. There is no information about possible countermeasures known. It may be suggested to	Protected by core rules.	Detected by scanner as SQL Injection attack.

				replace the affected object with an alternative product.		
10	URI Argument Injection	CVE-2021-38112	Amazon WorkSpaces Client workspaces URI argument injection	A vulnerability classified as critical has been found in Amazon WorkSpaces Client up to 3.1.8 on Windows. This affects an unknown code block of the component workspaces URI. The manipulation of the argument gpu-launcher with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-88. This is going to have an impact on confidentiality, integrity, and availability.	Protected by custom rules.	NA

11	Wordpress	CVE-2021-34621	ProfilePress Plugin up to 3.1.3 on WordPress User Registration RegistrationAuth. php privileges management	A vulnerability was found in ProfilePress Plugin up to 3.1.3 on WordPress (WordPress Plugin). It has been rated as critical. Affected by this issue is an unknown code of the file ~/src/Classes/Regist rationAuth.php of the component User Registration. The manipulation with an unknown input leads to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-269. Impacted is confidentiality, integrity, and availability.	Protected by custom rules.	NA
12	Cross Site Scripting	CVE-2021-30119	Kaseya VSA up to 9.5.6 cross site scripting [CVE-2021-30119]	A vulnerability was found in Kaseya VSA up to 9.5.6 and classified as problematic. This issue affects an unknown part. Upgrading to version 9.5.7 eliminates this vulnerability.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2021-24591	Highlight Plugin up to 0.9.2 on WordPress CustomCSS Setting cross site scripting	A vulnerability was found in Highlight Plugin up to 0.9.2 on WordPress. It has been classified as problematic. Affected is an unknown functionality of the component. Upgrading to version 0.9.3 eliminates this vulnerability.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2021-24724	MotoPress Timetable and Event Schedule Plugin up to 2.3.18 on WordPress cross site scripting	A vulnerability classified as problematic has been found in MotoPress Timetable and Event Schedule Plugin up to 2.3.18 on WordPress. This affects an unknown code of the component. Upgrading to version 2.3.19 eliminates this vulnerability.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2021-39320	Reflected XSS in underConstructio n Plugin	A vulnerability, which was classified as problematic, has been found in underConstruction plugin up to 1.18 on WordPress (WordPress Plugin). Affected by this issue is an unknown code block of the file ucOptions.php. The manipulation of the argument $GLOBALS['PHP_SEL F'] with an unknown input leads 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 scanner as Cross Site Scripting attack.

	CVE-2021-39322	Reflected XSS in Easy Social Icons	A vulnerability, which was classified as problematic, was found in Easy Social Icons Plugin up to 3.0.8 on WordPress (WordPress Plugin). Affected is the function $_SERVER['PHP_SELF']. The manipulation with an unknown input leads 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.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.