Weekly Zero-Day Vulnerability Coverage Bulletin

January 2021

Total Zero Day Vulnerabilities found: 16

Command Injection	Cross site request forgery	Directory Traversal	DOS Attack	Local File Inclusion	SQL Injection	Cross Site Scripting	WordPress
3	3	1	1	1	1	5	1

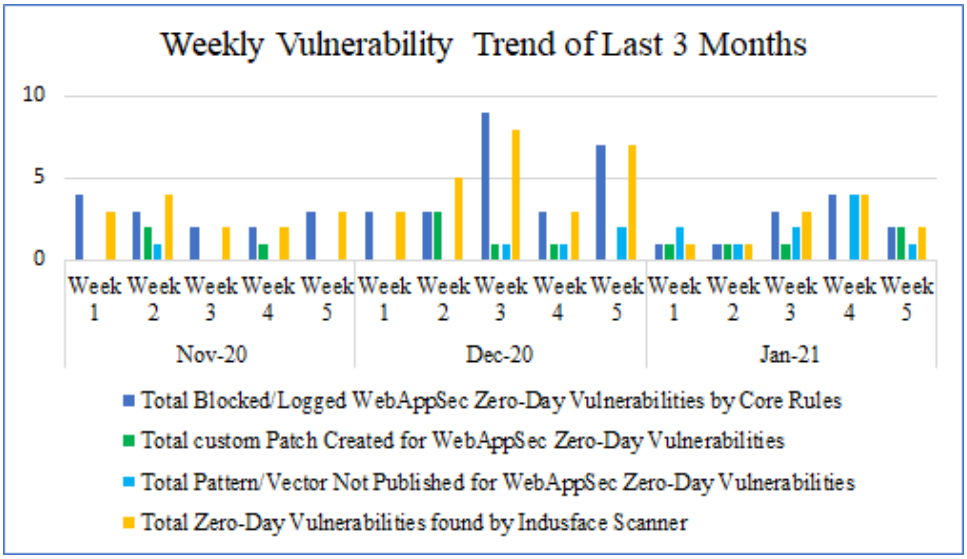
Zero-Day Vulnerabilities Protected through Core Rules	11
Zero-Day Vulnerabilities Protected through Custom Rules	5 *
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	11

* 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:

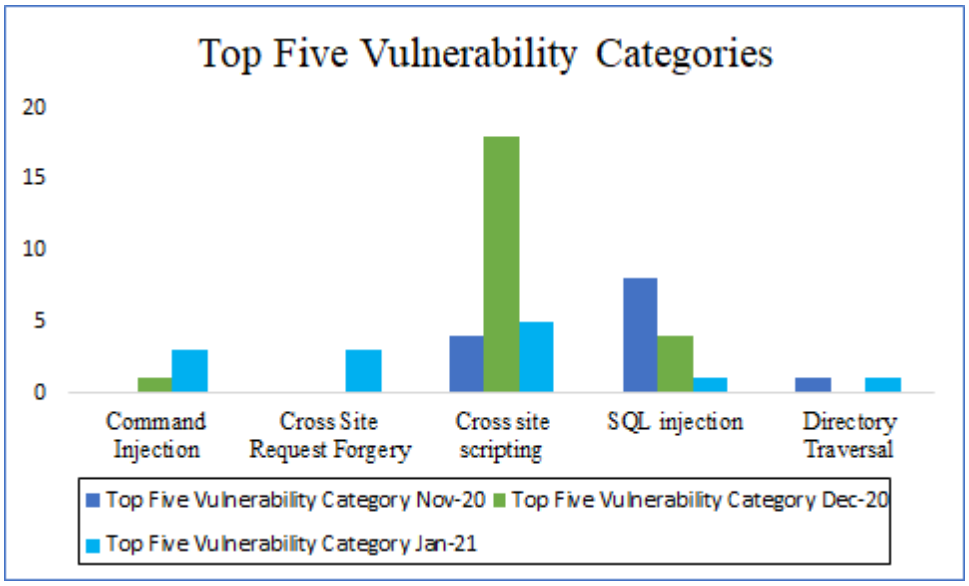
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



69% 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

69% 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-2020-23630	zzcms ver201910 Cookie sql injection	A blind SQL injection vulnerability exists in zzcms ver201910 based on time (cookie injection).	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2020-28480	jointjs Package up to 3.2.x util.setByPath code injection	The package jointjs before 3.3.0 are vulnerable to Prototype Pollution via util.setByPath (https://resources.jointjs.com/docs/jointjs/v3.2/joint.htmlutil.setByPath). The path used the access the object's key and set the value is not properly sanitized, leading to a Prototype Pollution.	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2020-20269	Caret Editor up to 4.0.0-rc21 Markdown Document Remote Code Execution	A specially crafted Markdown document could cause the execution of malicious JavaScript code in	Protected by core rules.	Detected by scanner as Command Injection attack.

				Caret Editor before 4.0.0-rc22.		
2	Cross Site Request Forgery	CVE-2020-36191	JupyterHub 1.1.0 Admin Panel /hub/api/user cross-site request forgery	JupyterHub 1.1.0 allows CSRF in the admin panel via a request that lacks an _xsrf field, as demonstrated by a /hub/api/user request (to add or remove a user account).	Protected by custom rules.	NA
		CVE-2020-35944	PageLayer Plugin up to 1.1.1 on WordPress pagelayer_settings_page cross-site request forgery	An issue was discovered in the PageLayer plugin before 1.1.2 for WordPress. The pagelayer_settings_page function is vulnerable to CSRF, which can lead to XSS.	Protected by custom rules.	NA
		CVE-2020-35942	NextGen Gallery, Critical vulnerability fixed in WordPress plugin with 800K installs	A Cross-Site Request Forgery (CSRF) issue in the NextGEN Gallery plugin before 3.5.0 for WordPress allows File Upload and Local File Inclusion via settings modification, leading to Remote Code Execution and XSS. (It is possible to bypass CSRF protection by simply not including a nonce parameter.)	Protected by custom rules.	NA

3	Directory Traversal/File Inclusion	CVE-2021-21269	Keymaker up to 0.1.x Assets Endpoint join path traversal	Keymaker is a Mastodon Community Finder based Matrix Community serverlist page Server. In Keymaker before version 0.2.0, the assets endpoint did not check for the extension. The rust `join` method without checking user input might have made it abe to do a Path Traversal attack causing to read more files than allowed. This is fixed in version 0.2.0.	Protected by core rules.	Detected by scanner as Directory Traversal attack.
4	DOS Attack	NA	Microsoft Remote Desktop Protocol (RDP) Reflection/Amplification DDoS Attack Mitigation Recommendations - January 2021	The Microsoft Remote Desktop Protocol (RDP) service included in Microsoft Windows operating systems is intended to provide authenticated remote virtual desktop infrastructure (VDI) access to Windows-based workstations and servers. The RDP service can be configured by Windows systems administrators to run on TCP/3389 and/or UDP/3389	Protected by custom rules.	Detected by scanner as Dos attack.
5	Local File Inclusion	CVE-2020-36193	Drupal Updates Patch Another Vulnerability Related to Archive Files	Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.	Protected by core rules.	Detected by scanner as Local File Inclusion attack.

6	SQL Injection	CVE-2021-3110	PrestaShop 1.7.7.0 id_products sql injection	The store system in PrestaShop 1.7.7.0 allows time-based boolean SQL injection via the module=productcomments controller=CommentGrade id_products[] parameter.	Protected by core rules.	Detected by scanner as SQL Injection attack.
7	WordPress	CVE-2020-25213	File Manager in the Wild Exploits for WordPress Vulnerability	The File Manager (wp-file-manager) plugin before 6.9 for WordPress allows remote attackers to upload and execute arbitrary PHP code because it renames an unsafe example El Finder connector file to have the .php extension. This, for example, allows attackers to run the elFinder upload (or mkfile and put) command to write PHP code into the wp-content/plugins/wp-file-manager/lib/files/ directory. This was exploited in the wild in August and September 2020.	Protected by core rules.	Detected by scanner as WordPress.
8	Cross Site Scripting	CVE-2020-35936	Post Grid Plugin up to 2.0.72 on WordPress AJAX post_grid_import_xml_layouts source cross site scripting	Stored Cross-Site Scripting (XSS) vulnerabilities in the Post Grid plugin before 2.0.73 for WordPress allow remote authenticated attackers to import layouts including JavaScript supplied via a remotely hosted crafted payload in the source parameter via AJAX. The action must be set to post_grid_import_xml_layouts.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2020-13959	Undisclosed Apache Velocity XSS vulnerability impacts GOV sites	The default error page for VelocityView in Apache Velocity Tools prior to 3.1 reflects back the vm file that was entered as part of the URL. An attacker can set an XSS payload file as this vm file in the URL which results in this payload being executed. XSS vulnerabilities allow attackers to execute arbitrary JavaScript in the context of the attacked website and the attacked user. This can be abused to steal session cookies, perform requests in the name of the victim or for phishing attacks.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	NA	Oracle Business Intelligence Enterprise Edition 11.1.1.7.140715 - Stored XSS	Oracle Business Intelligence Enterprise Edition 11.1.1.7.140715 - Stored XSS	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2021-25295	OpenCATS up to 0.9.5-3 cross site scripting [CVE-2021-25295]	OpenCATS through 0.9.5-3 has multiple Cross-site Scripting (XSS) issues.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	NA	MyBB 1.8.26 Released — Security Release	Cross-site Scripting (XSS) vulnerability in MyBB before 1.8.26 via Nested Auto URL when parsing messages.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.