Weekly Zero-Day Vulnerability Coverage Bulletin

April 2021

Total Zero Day Vulnerabilities found: 23

Command Injection	Cross Site Request forgery	Directory Traversal	DOS Attack	File Injection	Malicious File upload	SQL Injection	Cross Site scripting	External Entity Attack
2	2	6	1	3	1	3	3	2

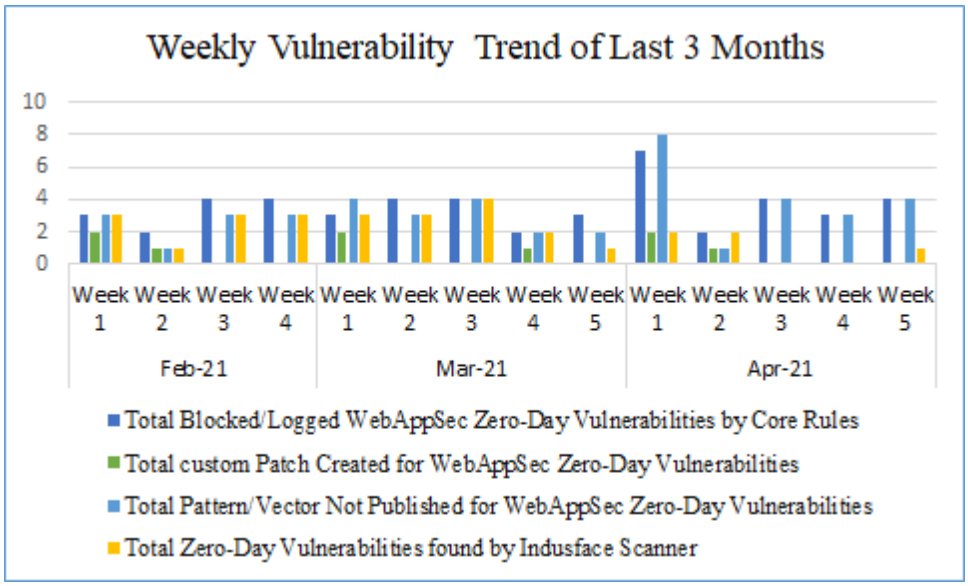
Zero-Day Vulnerabilities Protected through Core Rules	20
Zero-Day Vulnerabilities Protected through Custom Rules	3*
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	20

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

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

Vulnerability Trend:

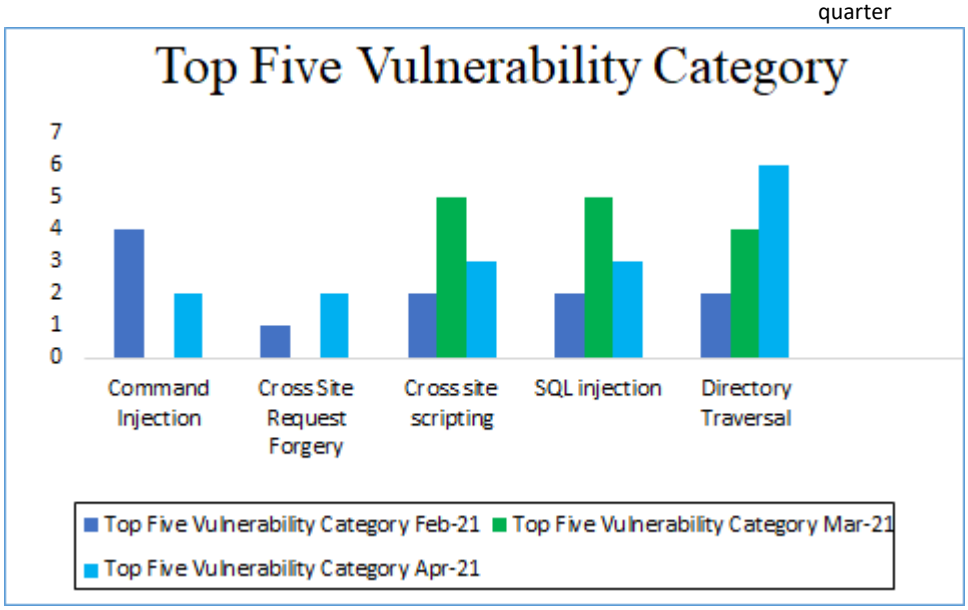
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



87% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

13% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

87% 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-2020-7857	Tobesoft XPlatform prior 9.2.2.280 command injection [CVE-2020-7857]	A vulnerability of XPlatform could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient validation of improper classes. This issue affects: Tobesoft XPlatform versions prior to 9.2.2.280.	Protected by Core rules.	Detected by scanner as Command Injection attack.
		CVE-2020-7034	Avaya Session Border Controller for Enterprise up to 8.1.1.x Message os	A command injection vulnerability in Avaya Session Border Controller for Enterprise could allow an authenticated, remote attacker to	Protected by Core rules.	Detected by scanner as Command Injection attack.

			command injection	send specially crafted messages and execute arbitrary commands with the affected system privileges. Affected versions of Avaya Session Border Controller for Enterprise include 7.x, 8.0 through 8.1.1.x		
2	Cross Site Request Forgery	CVE-2021-21641	Promoted Builds Plugin	A cross-site request forgery (CSRF) vulnerability in Jenkins promoted builds Plugin 3.9 and earlier allows attackers to promote builds.	Protected by Core rules.	NA
		CVE-2021-22512	Micro Focus Application Automation Tools Plugin up to 6.7 on Jenkins cross-site request forgery	Cross-Site Request Forgery (CSRF) vulnerability in Micro Focus Application Automation Tools Plugin - Jenkins plugin. The vulnerability affects version 6.7 and earlier versions. The vulnerability could allow form validation without permission checks.	Protected by Core rules.	NA

3	Directory Traversal/File Inclusion	CVE-2021-28918	Improper input validation of octal strings in netmask npm package	Improper input validation of octal strings in netmask npm package v1.0.6 and below allows unauthenticated remote attackers to perform indeterminate SSRF, RFI, and LFI attacks on many of the dependent packages. A remote unauthenticated attacker can bypass packages relying on netmask to filter IPs and reach critical VPN or LAN hosts.	Protected by Core rules.	Detected by scanner as Directory Traversal attack.
		CVE-2021-29418	The netmask package before 2.0.1 for Node.js mishandles certain unexpected characters	The netmask package before 2.0.1 for Node.js mishandles certain unexpected characters in an IP address string, such as an octal digit of 9. This (in some situations) allows attackers to bypass access control that is based on IP addresses. NOTE: this issue exists because of an incomplete fix for CVE-2021-28918.	Protected by Core rules.	Detected by scanner as Directory Traversal attack.
		CVE-2021-29424	The Net::Netmask module before 2.0000 for Perl does not properly consider extraneous zero characters at the beginning of an IP address string	The Net::Netmask module before 2.0000 for Perl does not properly consider extraneous zero characters at the beginning of an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses.	Protected by Core rules.	Detected by scanner as Directory Traversal attack.
		CVE-2021-29658	vscode-rufo Extension up to 0.0.3 on Visual Studio Binary	The unofficial vscode-rufo extension before 0.0.4 for Visual Studio Code allows attackers to execute arbitrary	Protected by Core rules.	Detected by scanner as Directory Traversal attack.

		Remote Code Execution	binaries if the user opens a crafted workspace folder.		
	CVE-2018-13379	Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks	An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 and FortiProxy 2.0.0, 1.2.0 to 1.2.8, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 under SSL VPN web portal allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.	Protected by Core rules.	Detected by scanner as Directory Traversal attack.
	NA	Zoom zero-day discovery	Pwn2Own is a high profile event organized by the Zero Day Initiative that challenges hackers to find serious new vulnerabilities in commonly used software and mobile devices. The event is held to demonstrate that popular software and devices come with flaws and vulnerabilities, and offers a counterweight to the underground trade in vulnerabilities.	Protected by Core rules.	Detected by scanner as Directory Traversal attack.

4	Dos attack	CVE-2021-29933	insert_many Crate up to 2021-01-26 on Rust a .next denial of service	An issue was discovered in the insert_many crate through 2021-01-26 for Rust. Elements may be dropped twice if a .next() method panics.	Protected by custom rules.	NA
5	File Injection	CVE-2019-11510	Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks	In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.	Protected by core rules.	Detected by scanner as Remote File Inclusion attack.
		CVE-2019-19781	Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	Protected by core rules.	Detected by scanner as Remote File Inclusion attack.
		NA	Widespread Attacks Continue Targeting Vulnerabilities in The Plus Addons for Elementor Pro	Widespread Attacks Continue Targeting Vulnerabilities in The Plus Addons for Elementor Pro	Protected by Core rules.	Detected by scanner as Remote File Inclusion attack.

6	Malicious File Upload	CVE-2021-24284	Remove Kaswara Modern WPBakery Page Builder Addons Plugin Immediately	The Kaswara Modern VC Addons WordPress plugin through 3.0.1 allows unauthenticated arbitrary file upload via the 'uploadFontIcon' AJAX action. The supplied zipfile being unzipped in the wp-content/uploads/kaswara/fonts_icon directory with no checks for malicious files such as PHP.	Protected by custom rules.	Detected by scanner as Malicious file upload attack.
7	SQL injection	CVE-2021-28245	PbootCMS up to 3.0.4 index.php search sql injection	PbootCMS 3.0.4 contains a SQL injection vulnerability through index.php via the search parameter that can reveal sensitive information through adding an admin account.	Protected by Core rules.	Detected by scanner as SQL Injection attack.
		CVE-2021-31856	Layer5 0.5.2 REST API meshery_pattern_persister.go order sql injection	A SQL Injection vulnerability in the REST API in Layer5 Meshery 0.5.2 allows an attacker to execute arbitrary SQL commands via the /experimental/patternfiles endpoint (order parameter in GetMesheryPatterns in models/meshery_pattern_persister.go).	Protected by Core rules.	Detected by scanner as SQL Injection attack.

		NA	SQL Injection Vulnerability Patched in CleanTalk AntiSpam Plugin	On March 4, 2021, the Wordfence Threat Intelligence team initiated responsible disclosure for a Time-Based Blind SQL Injection vulnerability discovered in Spam protection, AntiSpam, FireWall by CleanTalk, a WordPress plugin installed on over 100,000 sites. This vulnerability could be used to extract sensitive information from a site's database, including user emails and password hashes, all without logging into the site. We initially reached out to the plugin's developer on March 4, 2021 and sent over the full disclosure on March 5, 2021. A patched version of the plugin, 5.153.4, was released on March 10, 2021. Wordfence Premium users received firewall rules protecting against this vulnerability on March 4, 2021. Sites still running the free version of Wordfence received the same protection on April 3, 2021.	Protected by Core rules.	Detected by scanner as SQL Injection attack.
8	Cross Site Scripting	CVE-2020-13672	Drupal core - Critical - Cross-site scripting - SA-CORE-2021-002	Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances.	Protected by Core rules.	Detected by scanner as Cross Site Scripting attack.

		CVE-2021-25894	Magnolia CMS login.html mgnlUserId cross site scripting	Magnolia CMS from 6.1.3 to 6.2.3 contains a stored cross-site scripting (XSS) vulnerability in the /magnoliaPublic/travel/members/login.html mgnlUserId parameter.	Protected by Core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2021-30125	Webiness Jamf Pro up to 10.27.x Inventory History cross site scripting	Jamf Pro before 10.28.0 allows XSS related to inventory history, aka PI-009376.	Protected by Core rules.	Detected by scanner as Cross Site Scripting attack.
9	External Entity Attack	CVE-2021-29447	WordPress 5.7.1 Patches XXE Flaw in PHP 8	Wordpress is an open-source CMS. A user with the ability to upload files (like an Author) can exploit an XML parsing issue in the Media Library leading to XXE attacks. This requires WordPress installation to be using PHP 8. Access to internal files is possible in a successful XXE attack. This has been patched in WordPress version 5.7.1, along with the older affected versions via a minor release. We strongly recommend you keep auto-updates enabled.	Protected by Core rules.	Detected by scanner as external entity attack.
		CVE-2019-9670	Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks	mailboxd component in Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10 has an XML External Entity injection (XXE) vulnerability.	Protected by Core rules.	Detected by scanner as external entity attack.