Weekly Zero-Day Vulnerability Coverage Bulletin

May 2021

Total Zero Day Vulnerabilities found: 24

Command Injection	Cross site request forgery	Directory Traversal	SQL Injection	Cross Site Scripting	WordPress
4	5	1	3	9	2

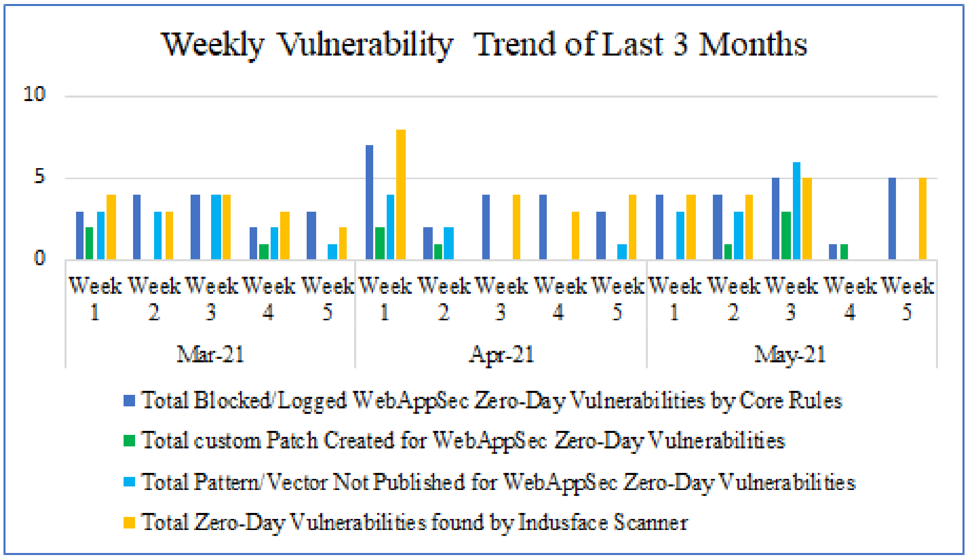
Zero-Day Vulnerabilities Protected through Core Rules	19
Zero-Day Vulnerabilities Protected through Custom Rules	5 *
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	19

* 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:

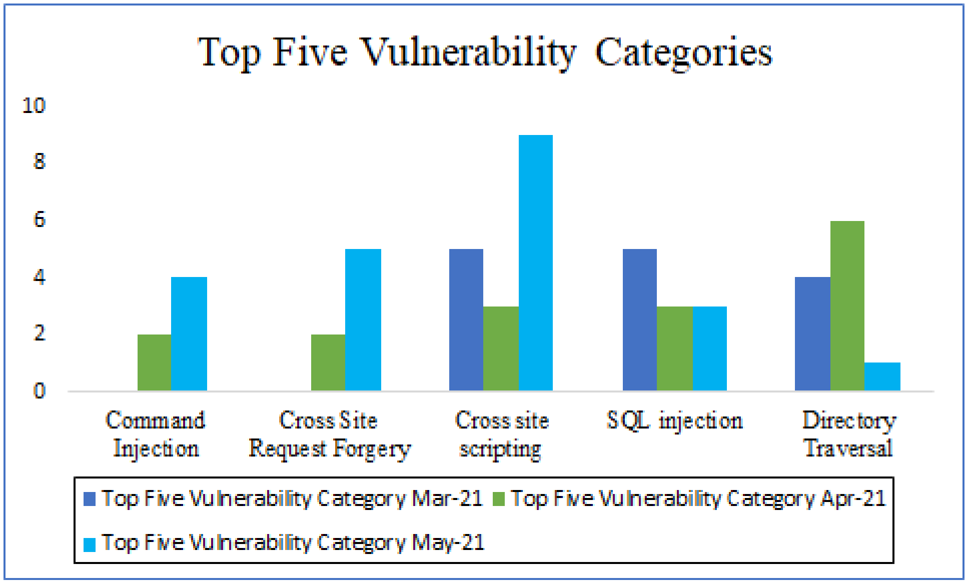
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



79% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

21% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

79% 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-2021-21527	Dell EMC PowerScale OneFS up to 9.1.0 os command injection [CVE-2021-21527]	Dell PowerScale OneFS 8.1.0-9.1.0 contain an improper neutralization of special elements used in an OS command vulnerability. This vulnerability may allow an authenticated user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE privileges to escalate privileges.	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2021-32563	Thunar up to 4.16.6/4.17.1 Command-Line	An issue was discovered in Thunar before 4.16.7 and	Protected by core rules.	Detected by scanner as Command

		Argument command injection	4.17.x before 4.17.2. When called with a regular file as a command-line argument, it delegates to a different program (based on the file type) without user confirmation. This could be used to achieve code execution.		Injection attack.
	CVE-2021-32605	ZZZCMS zzzphp up to 2.0.3 ?location=search keys os command injection	zzzcms zzzphp before 2.0.4 allows remote attackers to execute arbitrary OS commands by placing them in the keys parameter of a ?location=search URI, as demonstrated by an OS command within an "if" "end if" block.	Protected by core rules.	Detected by scanner as Command Injection attack.
	NA	Critical 21Nails Exim bugs expose millions of servers to attacks	MTA servers such as Exim are an easy target to attacks given that, in most cases, they are reachable over the Internet and provide attackers with a simple entry point into a target's network."Once exploited, they could modify sensitive email settings on the mail servers, allow adversaries to create new accounts on the target mail servers," Qualys explained.	Protected by core rules.	Detected by scanner as Command Injection attack.

2	Cross Site Request Forgery	CVE-2021-29238	CODESYS Automation Server up to 1.15.x cross-site request forgery	CODESYS Automation Server before 1.16.0 allows cross-site request forgery (CSRF).	Protected by custom rules.	NA
		CVE-2020-23376	NoneCMS 1.3 add.html name cross-site request forgery	NoneCMS v1.3 has a CSRF vulnerability in public/index.php/admin/nav/add.html, as demonstrated by adding a navigation column which can be injected with arbitrary web script or HTML via the name parameter to launch a stored XSS attack.	Protected by custom rules.	NA
		CVE-2020-18964	PHPOK 5.2.060 admin.php cross-site request forgery	A Cross Site Request Forgery (CSRF) vulnerability exists in PHPOK 5.2.060 via admin.php?c=admin&f=save, which could let a remote malicious user execute arbitrary code.	Protected by custom rules.	NA
		CVE-2021-34619	ForestBlog cross-site request forgery [CVE-2020-18964]	Cross Site Request Forgery (CSRF) Vulnerability in ForestBlog latest version via the website Management background, which could let a remote malicious gain privilege.	Protected by custom rules.	NA

	CVE-2021-34619	High Severity Vulnerability Patched in WooCommerce Stock Manager Plugin	the Wordfence Threat Intelligence team initiated the responsible disclosure process for a vulnerability that we discovered in WooCommerce Stock Manager; a WordPress plugin installed on over 30,000 sites. This flaw made it possible for an attacker to upload arbitrary files to a vulnerable site and achieve remote code execution, as long as they could trick a site's administrator into performing an action like clicking on a link.We initially reached out to the plugin's developer on May 21, 2021. After receiving confirmation of an appropriate communication channel, we provided the full disclosure details on May 24, 2021. A patch was quickly released on May 28, 2021 in version 2.6.0.	Protected by core rules.	NA

3	Directory Traversal/File Inclusion	CVE-2021-29472	PHP Composer Flaw That Could Affect Millions of Sites Patched	Composer is a dependency manager for PHP. URLs for Mercurial repositories in the root composer.json and package source download URLs are not sanitized correctly. Specifically crafted URL values allow code to be executed in the HgDriver if hg/Mercurial is installed on the system. The impact to Composer users directly is limited as the composer.json file is typically under their own control and source download URLs can only be supplied by third party Composer repositories they explicitly trust to download and execute source code from, e.g. Composer plugins. The main impact is to services passing user input to Composer, including Packagist.org and Private Packagist. This allowed users to trigger remote code execution. The vulnerability has been patched on Packagist.org and Private Packagist within 12h of receiving the initial vulnerability report and based on a review of logs, to the best of our knowledge, was not abused by anyone. Other services/tools using VcsRepository/VcsDriver or derivatives may	Protected by core rules.	Detected by scanner as Directory Traversal attack.

				also be vulnerable and should upgrade their composer/composer dependency immediately. Versions 1.10.22 and 2.0.13 include patches for this issue.		
4	SQL Injection	CVE-2020-15153	Ampache up to 4.2.1 sql injection	Ampache before version 4.2.2 allows unauthenticated users to perform SQL injection. Refer to the referenced GitHub Security Advisory for details and a workaround. This is fixed in version 4.2.2 and the development branch.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		NA	JET engine flaws can crash Microsoft's IIS, SQL Server, say Palo Alto researchers	A trio of researchers at Palo Alto Networks has detailed vulnerabilities in the JET database engine, and demonstrated how those flaws can be exploited to ultimately execute malicious code on systems running Microsoft's SQL Server and Internet Information Services web server.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2021-24340	Over 600,000 Sites Impacted by WP Statistics Patch	The WP Statistics WordPress plugin before 13.0.8 relied on using the WordPress esc_sql() function on a field not delimited by quotes and did not first prepare the query. Additionally, the page, which should have been accessible to administrator only, was also available to any visitor, including unauthenticated ones.	Protected by core rules.	Detected by scanner as SQL Injection attack.

5	WordPress	CVE-2021-24370	Critical 0-day in Fancy Product Designer Under Active Attack	The WordPress plugin Easy FancyBox is prone to a stored cross-site scripting (XSS) vulnerability. The vulnerability exists within the Settings Menu in inc/class-easyfancybox.php due to improper encoding of arbitrarily submitted settings parameters. This occurs because there is no inline styles output filter. Successful exploitation would allow an authenticated attacker to inject arbitrary HTML and JavaScript into the site.	Protected by core rules.	Detected by scanner as Wordpress easy fancybox.
		CVE-2021-24352	Severe Vulnerabilities Patched in Simple 301 Redirects by BetterLinks Plugin	The export_data function of the Simple 301 Redirects by BetterLinks WordPress plugin before 2.0.4 had no capability or nonce checks making it possible for unauthenticated users to export a site's redirects.	Protected by Custom rules.	NA

6	Cross Site Scripting	CVE-2020-18084	yzmCMS 5.2 /member/index/login.html referer cross site scripting	Cross Site Scripting (XSS) in yzmCMS v5.2 allows remote attackers to execute arbitrary code by injecting commands into the "referer" field of a POST request to the component "/member/index/login.html" when logging in.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2021-31792	SuiteCRM up to 7.11.18 Client Account Page name cross site scripting	XSS in the client account page in SuiteCRM before 7.11.19 allows an attacker to inject JavaScript via the name field	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2021-24270	DeTheme Kit for Elementor Plugin up to 1.5.5.4 on c Widget cross site scripting	The “DeTheme Kit for Elementor” WordPress Plugin before 1.5.5.5 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2021-20717	EC-CUBE 4.0.0 up to 4.0.5 EC Web Site cross site scripting	Cross-site scripting vulnerability in EC-CUBE 4.0.0 to 4.0.5 allows a remote attacker to inject a specially crafted script in the specific input field of the EC web site which is created using EC-CUBE. As a result, it may lead to an arbitrary script execution on the administrator's web browser.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack. NA

	CVE-2021-34620	Cross-Site Request Forgery Patched in WP Fluent Forms	the Wordfence Threat Intelligence team responsibly disclosed a Cross-Site Request Forgery (CSRF) vulnerability in WP Fluent Forms, a WordPress plugin installed on over 80,000 sites. This vulnerability also allowed a stored Cross-Site Scripting(XSS) attack which, if successfully exploited, could be used to take over a site.We reached out to the plugin developer, WP Manage Ninja, on March 2, 2021 and received a response within 24 hours. We sent over the full disclosure on March 3, 2021, and a patched version of the plugin, 3.6.67, was released on March 5, 2021.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2021-26032	Joomla CMS up to 3.9.26 MediaHelper::canUpload cross site scripting	An issue exists in Joomla! 3.0.0 up to and including 3.9.26. HTML was missing in the executable block list of MediaHelper::canUpload, leading to XSS attack vectors.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2021-33469	PHPGurukul COVID19 Testing Management System 1.0 Parameter Admin name cross site scripting	COVID19 Testing Management System 1.0 is vulnerable to Cross Site Scripting (XSS) via the "Admin name" parameter.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2020-18229	PHPMyWind 5.5 web_config.php&amp cfg_copyright cross site scripting	Cross Site Scripting (XSS) in PHPMyWind v5.5 allows remote attackers to execute arbitrary code by injecting scripts into the parameter "$cfg_copyright" of component " /admin/web_config.php".	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	NA	Joomla Content System Vulnerable to Multiple Flaws	Joomla is a widely used CMS system with more than 1.5 million installations. The researchers note one of the identified vulnerabilities is a password reset flaw and another is a cross-site scripting - or XSS - vulnerability that can lead to privilege escalation.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.