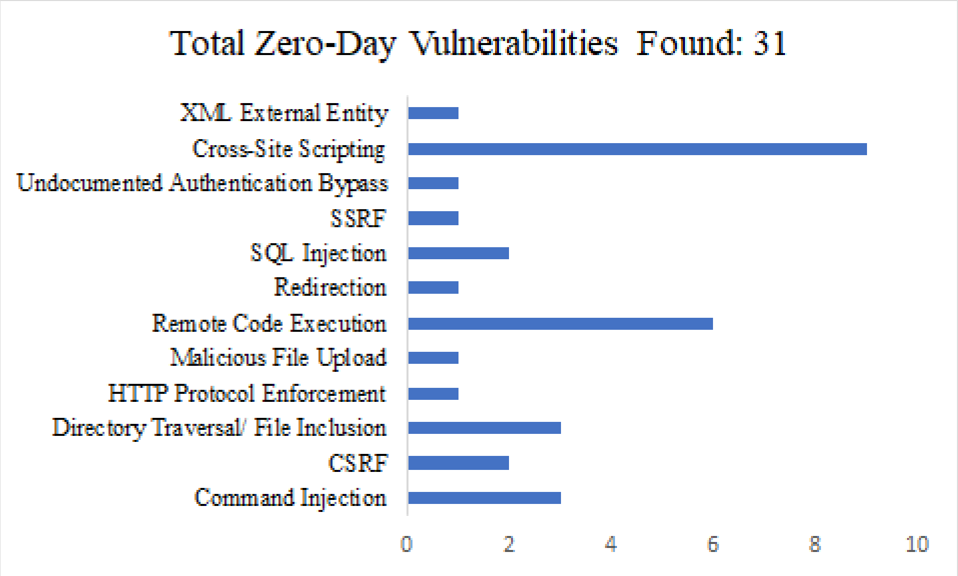
Monthly Zero-Day Vulnerability Coverage Bulletin

July 2021



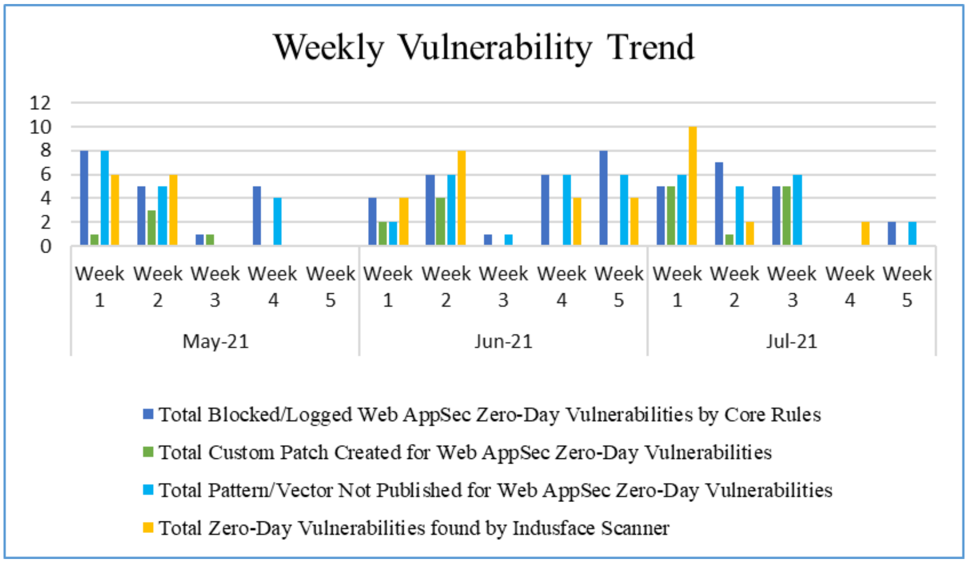
Zero-Day vulnerabilities protected through core rules	19
Zero-Day vulnerabilities protected through custom rules	11 *
Zero-Day vulnerabilities for which protection cannot be determined	1 **
Zero-Day vulnerabilities found by Indusface WAS	18

* 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:

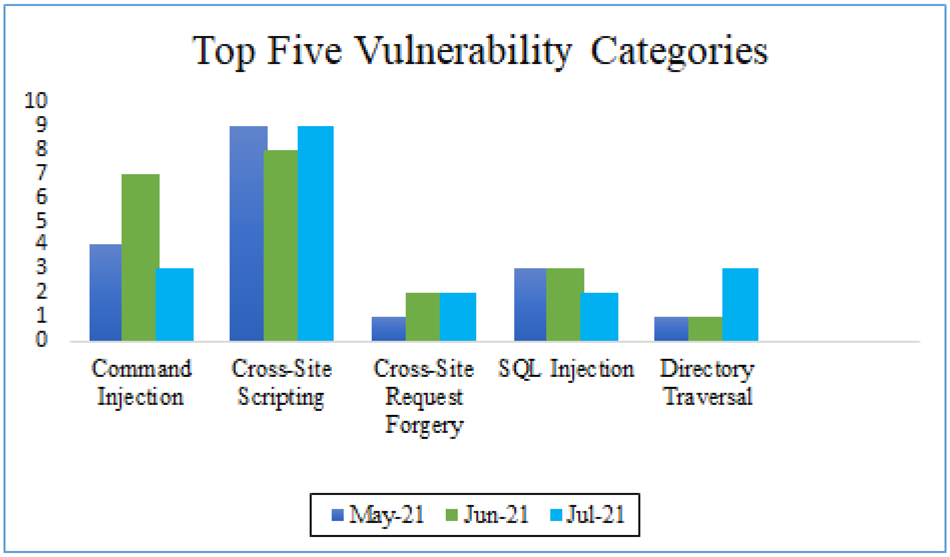
The weekly trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



61% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

36% of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

58% 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-2021-22123	Fortinet FortiWeb OS Command Injection	An OS command injection vulnerability in FortiWeb's management interface (version 6.3.11 and prior) can allow a remote, authenticated attacker to execute arbitrary commands on the system, via the SAML server configuration page. This is an instance of CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') and has a CVSSv3 base score of 8.7. This vulnerability appears to be related to CVE-2021-22123	Protected by core rules.	Detected by the scanner as the Command Injection attack.
		NA	RCE Vulnerability in cdnjs	cdnjs provides JavaScript, CSS, images, and fonts assets for websites to reference with more than 4,000 libraries available. By utilizing cdnjs, websites can load faster with less strain on one's own origin server as files are served directly. This vulnerability allowed the researcher to execute arbitrary code, granting the	Protected by core rules.	Detected by the scanner as the Command Injection attack.

			ability to modify assets.		
	CVE-2020-36239	Critical Jira Flaw in Atlassian Could Lead to RCE	A vulnerability classified as critical was found in Atlassian Jira Data Center, Jira Core Data Center, Jira Software Data Center, and Jira Service Management Data Center (Bug Tracking Software) (the affected version is unknown). This vulnerability affects an unknown function of the part Eh cache RMI. The manipulation with an unknown input led to a privilege escalation vulnerability. Th CWE definition for the vulnerability is CWE-502. 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.

2	Cross-Site Request Forgery	CVE-2021-32730	XWi up to 12.10.4/13.1 cross-site request forgery [CVE-2021-32730]	A vulnerability, which was classified as problematic, was found in xwi. Affected is an unknown functionality. Upgrading to version 12.10.5 or 13.2RC1 eliminates this vulnerability. Applying a patch is able to eliminate this problem. The bugfix is ready for download. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by custom rules.	NA
		CVE-2020-36399	phpList up to 3.5.4 Bounce Rules rule1 cross site scripting	A vulnerability has been found in phpList and classified as problematic. Affected by this vulnerability is some unknown processing of the component. 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
3	Directory Traversal/File Inclusion	CVE-2021-24375	Motor Theme up to 3.0.x on WordPress path traversal	A vulnerability was found in Motor Theme on WordPress. It has been declared as critical. Affected by this vulnerability is the function. Upgrading to version 3.1.0 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Directory Traversal attack.
		CVE-2021-34638	Authenticated Directory Traversal	The WordPress Download Manager plugin allows the use of templates to	Protected by core rules	Detected by the scanner as the Directory

	change how download pages are displayed. Although there were some protections in place to protect against directory traversal, these were woefully insufficient. As such, it was possible for a user with lower permissions, such as a contributor, to retrieve the contents of a site's wp-config.php file by adding a new download and performing a directory traversal attack using the file[page_template] parameter. Upon previewing the download, the contents of the wp-config.php file would be visible in the page source. Since the contents of the file provided in the file[page_template] parameter were echoed out onto the page source, a user with author-level permissions could also upload a file with an image extension containing malicious JavaScript and set the contents of file[page_template] to the path of the uploaded file. This would lead to the JavaScript in the file being executed whenever the page was viewed or	Traversal attack.

			previewed resulting in Stored Cross-Site Scripting.		
	CVE-2021-33037	Apache Tomcat HTTP Header request smuggling	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.	Protected by core rules	Detected by the scanner as the Directory Traversal attack.

4	HTTP Protocol Enforcement	NA	HTTP Request Smuggling in Web Proxies	HTTP web proxies and web accelerators that support HTTP/2 for an HTTP/1.1 backend webserver are vulnerable to HTTP Request Smuggling. The affected systems allow invalid characters such as carriage return and newline characters in HTTP/2 headers. When an attacker passes these invalid contents to a vulnerable system, the forwarded HTTP/1 request includes the unintended malicious data. This is commonly known as HTTP Request Splitting. In the case of HTTP web proxies, this vulnerability can lead to HTTP Request smuggling, which enables an attacker to access protected internal sites.	Protected by core rules.	Detected by the scanner as the HTTP Request smuggling attack.

5	Malicious File Upload	NA	Vulnerable Plugin Exploited in Spam Redirect Campaign	Some weeks ago, a critical unauthenticated privilege escalation vulnerability was discovered in old, unpatched versions of the wp-user-avatar plugin. It also allows for arbitrary file uploads, which is where we have been seeing the infections start. This plugin has over 400,000 installations so we have seen a sustained campaign to infect sites with this plugin installed.	Protected by custom rules.	NA

6	Remote Code Execution (RCE)	CVE-2021-34473	Microsoft Exchange Server 2013 CU23/2016 CU19/2016 CU20/2019 CU8/2019 CU9 REMOTE CODE EXECUTION	A vulnerability was found in Microsoft Exchange Server 2013 CU23/2016 CU19/2016 CU20/2019 CU8/2019 CU9 (Groupware Software). It has been rated as very critical. Impacted is confidentiality, integrity, and availability. The weakness was disclosed 07/13/2021 as confirmed security guidance (Website). The advisory is shared at portal.msrc.microsoft.com. The identification of this vulnerability is CVE-2021-34473 since 06/09/2021. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation.	Protected by custom rules.	NA
		CVE-2021-34523	Microsoft Exchange Server 2013 CU23/2016 CU19/2016 CU20/2019 CU8/2019 CU9 unknown vulnerability	A vulnerability was found in Microsoft Exchange Server 2013 CU23/2016 CU19/2016 CU20/2019 CU8/2019 CU9 (Groupware Software). It has been declared as critical. As an impact it is known to affect confidentiality, and integrity.	Protected by custom rules.	NA

	CVE-2021-31207	Microsoft Exchange Server 2013 CU23/2016 CU19/2016 CU20/2019 CU8/2019 CU9 Privilege Escalation	A vulnerability classified as critical has been found in Microsoft Exchange Server 2013 CU23/2016 CU19/2016 CU20/2019 CU8/2019 CU9 (Groupware Software). This is going to have an impact on confidentiality, integrity, and availability.	Protected by custom rules.	NA
	CVE-2021-34639	Authenticated File Upload	WordPress Download Manager plugin patched a vulnerability allowing authors and other users with the upload_files capability to upload files with php4 extensions as well as other potentially executable files. While the patch in question was sufficient to protect many configurations, it only checked the very last file extension, so it was still possible to perform a “double extension” attack by uploading a file with multiple extensions. For instance, it was possible to upload a file titled info.php.png. This file would be executable on certain Apache/mod_php configurations that use an AddHandler or AddType directive.	Protected by Core Rules	Detected by the scanner as the remote code execution attack.

	CVE-2021-3129	Laravel (<=v8.4.2) exploit attempts for CVE-2021-3129	A vulnerability was found in Ignition up to 2.5.1. It has been declared as critical. This vulnerability affects the function file_get_contents/file_put_contents of the component Debug Mode. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was shared 01/13/2021. The advisory is available at ambionics.io. This vulnerability was named CVE-2021-3129 since 01/12/2021. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details are known, but there is no available exploit.	Protected by custom rules.	NA
	CVE-2019-2729	Oracle Warns of Critical Remotely Exploitable Weblogic Server Flaws	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic	Protected by custom rules.	NA

		Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8	

7	Redirection	CVE-2020-23182	PHP-Fusion 9.03.60 Shoutbox Message Panel shoutbox_archive.php redirect	A vulnerability, which was classified as problematic, was found in PHP-Fusion 9.03.60. This affects an unknown part of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Research queue	NA
8	SQL Injection	NA	Zero-Day Attacks on Critical WooCommerce Bug Threaten Databases	A critical SQL-injection security vulnerability in the WooCommerce e-commerce platform and a related plugin has been under attack as a zero-day bug, researchers have disclosed. The exploitation prompted WooCommerce to release an emergency patch for the issue late on Wednesday. The bug could allow unauthenticated cyberattackers to make off with scads of information from an online store’s database – anything from customer data and payment-card info to employee credentials.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-28423	PHPGurukul Teachers Record Management System 1.0 POST Parameter edit-subjects-detail.php editid sql injection	A vulnerability has been found inPHPGurukul Teachers Record Management System and classified as critical. Affected by this vulnerability is	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

				an unknown code block of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
9	SSRF	CVE-2021-35209	Server-Side Request Forgery (SSRF) in Zimbra	Zimbra is a popular webmail solution for global enterprises. Bypass of an allow-list that leads to a powerful Server-Side Request Forgery vulnerability (CVE-2021-35209). It can be exploited by an authenticated member of an organization with any permission role, which means that it can be combined with the XSS vulnerability.	Protected by custom rules.	Detected by the scanner as the SSRF Attack.
10	Undocumented Authentication Bypass	NA	Undocumented authentication bypass	Adobe Experience Manager (AEM) is a widely used content management solution for building digital customer experiences, like websites, mobile apps and forms. bug allows attackers to bypass authentication and gain access to Package Manager if the security controls for out-of-box protection are manually removed. This issue allows an unauthorized user to view and download packages.	Protected by custom rules.	NA

11	Cross-Site Scripting	NA	Exploiting Less.js to Achieve RCE	Less (less.js) is a preprocessor language that transpiles to valid CSS code. It offers functionality to help ease the writing of CSS for websites. Vulnerability is a result of the enhanced import feature of Less.js, which contains an inline mode that doesn't interpret the requested content. This can be used to request local or remote text content and return it in the resulting CSS.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		NA	MULTIPLE VULNERABILITIES IN CPANEL/WHM	cPanel is a web hosting control panel software developed by cPanel, LLC. It provides a graphical interface (GUI) and automation tools designed to simplify the process of hosting a web site to the website owner or the "end user". This XSS actually gives you the ability to escalate your privileges and execute commands on the server as root. Since cPanel/WHM allows you to execute shell commands from the browser, using web terminals (via websockets, details in the next paragraph) and we just XSSed the root user, it means we	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

			got RCE on the server as root.		
	CVE-2021-31721	Chevereto up to 3.17.0 Image Upload image title cross site scripting	A vulnerability was found in Chevereto up to 3.17.0. It has been rated as problematic. This issue affects an unknown code block of the component. Upgrading to version 3.17.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

	CVE-2021-35208	DOM-based Stored Cross-Site-Scripting (XSS) in Zimbra	Zimbra is a popular webmail solution for global enterprises. Cross-Site Scripting vulnerability (CVE-2021-35208) can be triggered in a victim's browser when viewing an incoming email. The malicious email would contain a crafted JavaScript payload that, when executed, would provide an attacker with access to all emails of the victim, as well as to their webmail session. With this, other features of Zimbra could be accessed and further attacks could be launched.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	CVE-2021-35360	dotCMS 21.05.1 dotAdmin/#/c/containers cross site scripting	A vulnerability has been found in dotCMS 21.05.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file. 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 Cross-Site Scripting attack.

	CVE-2021-34641	XSS Vulnerability Patched in SEOPress Affects 100,000 sites	A flaw in SEOPress that granted attackers the ability to inject arbitrary web scripts that could ultimately allow attackers to take over WordPress sites. This flaw has been fully patched in version 5.0.4. We recommend that WordPress users immediately update to the latest version available, which is version 5.0.4 at the time of this publication, if running a vulnerable version of this plugin.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
	NA	Drupal core - Moderately critical - Third-party libraries - SA-CORE-2021-005	Vulnerabilities are possible if Drupal is configured to allow use of the CKEditor library for WYSIWYG editing. An attacker that can create or edit content (even without access to CKEditor themselves) may be able to exploit one or more Cross-Site Scripting (XSS) vulnerabilities to target users with access to the WYSIWYG CKEditor, including site admins with privileged access.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

	CVE-2021-36026	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 Customer Address Upload cross site scripting	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 problematic. This affects an unknown part of the component Customer Address Upload Handler. The manipulation with an 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.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

		CVE-2021-36027	Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1 Form Field cross site scripting	A vulnerability was found in Adobe Magento Commerce up to 2.3.7/2.4.2/2.4.2-p1. It has been declared as problematic. This vulnerability affects an unknown code of the component Form Field Handler. The manipulation with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-79. As an impact it is known to 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.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
12	XML External Entity	CVE-2021-37425	XML External Entity Expansion in MobileTogether Server	A vulnerability in the MobileTogether server which allows users with access to at least one app to read arbitrary, non-binary files from the file system and perform server-side requests. The vulnerability can also be used to deny availability of the system.	Protected by custom rules	NA