Weekly Zero-Day Vulnerability Coverage Bulletin

June 2021

Total Zero Day Vulnerabilities found: 31

SQL Injection	Cross Site Scripting	Direct Traversal	PHP remote Code execution	Command Injection	Cross site request forgery	DOS attack	External Entity Attack
3	8	1	4	8	3	3	1

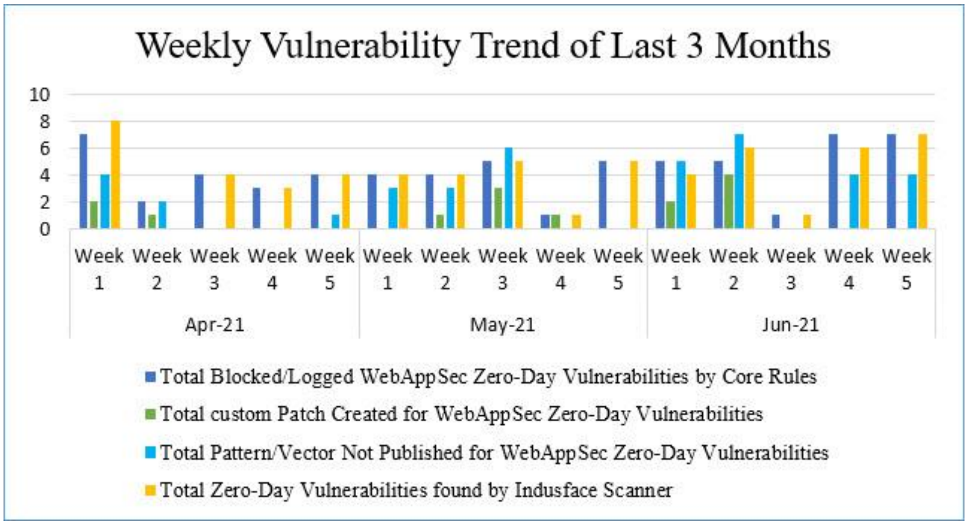
Zero-Day Vulnerabilities Protected through Core Rules	25
Zero-Day Vulnerabilities Protected through Custom Rules	6*
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	21

* 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:

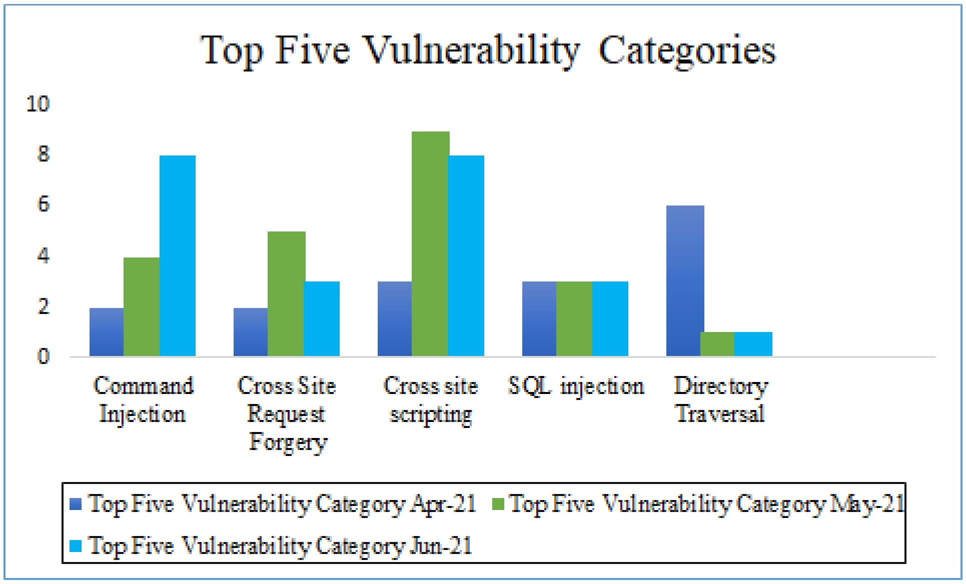
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



81% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

19% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

68% 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	SQL Injection	CVE-2020-18667	WebPort up to 1.19.1 Connection Parameter sql injection	SQL Injection vulnerability in WebPort <=1.19.1 via the new connection, parameter name in type-conn.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-23711	NavigateCMS 2.9 Input Category navigate.php sql injection	SQL Injection vulnerability in NavigateCMS 2.9 via the URL encoded GET input category in navigate.php.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-21394	Zhong Bang CRMEB Mall System 2.60/3.1 SystemDatabackup.php tablename sql injection	SQL Injection vulnerability in Zhong Bang Technology Co., Ltd CRMEB mall system V2.60 and V3.1 via the tablename parameter in SystemDatabackup.php.	Protected by core rules.	Detected by scanner as SQL Injection attack.

2	Cross Site Scripting	CVE-2020-27377	CMS Made Simple 2.2.14 Setting News Module cross site scripting	A cross-site scripting (XSS) vulnerability was discovered in the Administrator panel on the 'Setting News' module on CMS Made Simple 2.2.14 which allows an attacker to execute arbitrary web scripts.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-36139	BloofoxCMS 0.5.2.1 Parameter fileurl cross site scripting	BloofoxCMS 0.5.2.1 allows Reflected Cross-Site Scripting (XSS) vulnerability by inserting a XSS payload within the 'fileurl' parameter.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Prototype Pollution Vulnerabilities	JavaScript is a language implemented in nearly all web applications, from building rich client interfaces with frameworks like AngularJS to designing efficient backends using a NodeJS environment. For developers, there is a plethora of libraries available, and they are often used without any prior security assessment. Over the last few years, prototype pollution vulnerabilities have been discovered in many of these libraries, introducing serious security risks to applications utilizing them (see for example the security advisories issued for the Node Packet Manager packages). For example, the popular JavaScript library Lodash, used as a dependency by more than 140k packages, has been impacted by	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

			this bug referenced as CVE-2020-8203. From cross-site scripting (XSS) to remote code execution (RCE) attacks, malicious actors can conduct advanced exploitation scenarios with prototype pollution vulnerabilities.		
	CVE-2021-33829	Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2021-003	A cross-site scripting (XSS) vulnerability in the HTML Data Processor in CKEditor 4 4.14.0 through 4.16.x before 4.16.1 allows remote attackers to inject executable JavaScript code through a crafted comment because --!> is mishandled.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2021-23398	react-bootstrap-table dataFormat cross site scripting	All versions of package react-bootstrap-table are vulnerable to Cross-site Scripting (XSS) via the dataFormat parameter. The problem is triggered when an invalid React element is returned, leading to dangerouslySetInnerHTML being used, which does not sanitize the output.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-18671	RoundCube Mail up to 1.3.11/1.4.4 SMTP Configuration /installer/test.php cross site scripting	Cross Site Scripting (XSS) vulnerability in Roundcube Mail <=1.4.4 via smtp config in /installer/test.php.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2021-35501	PandoraFMS up to 7.54 Visual Console name cross site scripting	PandoraFMS <=7.54 allows Stored XSS by placing a payload in the name field of a visual console. When a user or an administrator visits the console, the XSS payload will be executed.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-28903	Trigger XSS by tainting data returned to Nagios Fusion from XI	The Nagios Fusion application periodically polls the fused Nagios XI servers to get information to display on various Fusion dashboards. The security model for doing this is inherently flawed since the Nagios Fusion will trust any data returned by the fused XI server. Since the data is trusted, the Nagios Fusion will display the information on various dashboards without sanitising the data. Therefore, by tainting data returned from the XI server under our control we can trigger Cross-Site Scripting and execute JavaScript code in the context of a Fusion user	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

3	Directory Traversal/File Inclusion	CVE-2021-20698	Sharp NEC UN462A HTTP Request Remote Privilege Escalation	Sharp NEC Displays (UN462A R1.300 and prior to it, UN462VA R1.300 and prior to it, UN492S R1.300 and prior to it, UN492VS R1.300 and prior to it, UN552A R1.300 and prior to it, UN552S R1.300 and prior to it, UN552VS R1.300 and prior to it, UN552 R1.300 and prior to it, UN552V R1.300 and prior to it, UX552S R1.300 and prior to it, UN552 R1.300 and prior to it, V864Q R2.000 and prior to it, C861Q R2.000 and prior to it, P754Q R2.000 and prior to it, V754Q R2.000 and prior to it, C751Q R2.000 and prior to it, V964Q R2.000 and prior to it, C961Q R2.000 and prior to it, P654Q R2.000 and prior to it, V654Q R2.000 and prior to it, C651Q R2.000 and prior to it, V554Q R2.000 and prior to it) allows an attacker to obtain root privileges and execute remote code by sending unintended parameters that contain specific characters in http request.	Protected by core rules.	Detected by scanner as Directory Traversal attack.

4	PHP Remote Code Execution	CVE-2021-20019	SonicWall bug that affected 800K firewalls was only partially fixed	CVE-2021-20019 is a buffer overflow vulnerability in SonicWall's SonicOS. A remote, unauthenticated attacker could exploit the flaw by sending a specially crafted HTTP request to a vulnerable SonicWall device. Successful exploitation of this vulnerability would result in a partial memory leak, disclosing sensitive internal information to the attacker. In a blog post, Young says that the information disclosed could include memory addresses that would be "useful information" for "exploiting an RCE bug	Protected by core rules.	NA
		CVE-2021-21985	Critical VMware vCenter Server Remote Code Execution	The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.	Protected by core Rules.	NA
		CVE-2020-28648	RCE on Nagios XI server from low privilege Nagios XI user	The first vulnerability we will look at is the Remote Code Execution on the Nagios XI server. This is an authenticated vulnerability but can be run from the context of a low privilege user.	Protected by Core Rules.	NA

		CVE-2020-28902	Elevate privileges from apache to root using the ‘cmd_subsys.php	With the ability to eval PHP code on the Fusion server we can run code as the apache user. As the apache user we can insert a malicious row into the fusion database commands table. This will abuse the command injection vulnerability in the cmd_subsys.php script that will execute code as the nagios user.	Protected by core rules.	NA
5	Command injection	CVE-2021-26471	Vembu BDR Suite up to 4.1.x GET Request command injection	Vembu BDR Suite before 4.2.0 allows Unauthenticated Remote Code Execution by placing a command in a GET request (issue 1 of 2).	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2021-20731	Buffalo WSR-1166DHP3/WSR-1166DHP4 os command injection [CVE-2021-20731]	WSR-1166DHP3 firmware Ver.1.16 and prior and WSR-1166DHP4 firmware Ver.1.02 and prior allow an attacker to execute arbitrary OS commands with root privileges via unspecified vectors.	Protected by core rules.	Detected by scanner as Command Injection attack.

	CVE-2020-7200	HPE fixes critical zero-day vulnerability	A remotely exploitable vulnerability exists within HPE System Insight Manager (SIM) version 7.6.x that can be leveraged by a remote unauthenticated attacker to execute code within the context of HPE System Insight Manager's hpsimsvc.exe process, which runs with administrative privileges. The vulnerability occurs due to a failure to validate data during the deserialization process when a user submits a POST request to the /simsearch/messagebroker/amfsecure page. This module exploits this vulnerability by leveraging an outdated copy of Commons Collection, namely 3.2.2, that ships with HPE SIM, to gain remote code execution as the administrative user running HPE SIM.	Protected by core rules.	Detected by scanner as Command Injection attack.
	CVE-2020-28910	Elevate privileges to 'root' on Nagios XI server	Creation of a Temporary Directory with Insecure Permissions in Nagios XI 5.7.5 and earlier allows for Privilege Escalation via creation of symlinks, which are mishandled in getprofile.sh.	Protected by core rules.	Detected by scanner as Command Injection attack.

	CVE-2021-20745	Inkdrop up to 5.3.0 Snippet os command injection	Inkdrop versions prior to v5.3.1 allows an attacker to execute arbitrary OS commands on the system where it runs by loading a file or code snippet containing an invalid iframe into Inkdrop.	Protected by core rules.	Detected by scanner as Command Injection attack.
	CVE-2021-33515	Dovecot up to 2.3.14 Submission command injection	The submission service in Dovecot before 2.3.15 allows STARTTLS command injection in lib-smtp. Sensitive information can be redirected to an attacker-controlled address	Protected by core rules.	Detected by scanner as Command Injection attack.
	CVE-2020-28905	Authenticated remote code execution on Nagios Fusion	Now that we have code execution from the context of a Nagios Fusion user we can exploit a vulnerability in the way Nagios Fusion handles table pagination to achieve RCE on the Fusion server. Table pagination refers to the functionality that presents table data to users in a paginated form. This allows a user to navigate the various pages and results in the browser.	Protected by core rules.	Detected by scanner as Command Injection attack.

		CVE-2021-33571	Django up to 2.2.23/3.1.11/3.2.3 access control [CVE-2021-33571]	In Django 2.2 before 2.2.24, 3.x before 3.1.12, and 3.2 before 3.2.4, URLValidator, validate_ipv4_address, and validate_ipv46_address do not prohibit leading zero characters in octal literals. This may allow a bypass of access control that is based on IP addresses. (validate_ipv4_address and validate_ipv46_address are unaffected with Python 3.9.5+..).	Protected by core rules.	Detected by scanner as Command Injection attack.
6	Cross Site Request Forgery	CVE-2020-36140	BloofoxCMS 0.5.2.1 cross-site request forgery [CVE-2020-36140]	BloofoxCMS 0.5.2.1 allows Cross-Site Request Forgery (CSRF) via 'mode=settings&page=editor', as demonstrated by use of 'mode=settings&page=editor' to change any file content (Locally/Remotely).	Protected by core rules.	NA.
		CVE-2021-26474	Vembu BDR Suite up to 4.1.x GET Request server-side request forgery	Vembu BDR Suite before 4.2.0 allows Unauthenticated SSRF via a GET request that specifies a hostname and port number.	Protected by custom rules.	NA
		CVE-2020-15377	Brocade SANnav up to 2.1.0 Webtools server-side request forgery	Webtools in Brocade SANnav before version 2.1.1 allows unauthenticated users to make requests to arbitrary hosts due to a misconfiguration; this is commonly referred to as Server-Side Request Forgery (SSRF).	Protected by custom rules.	NA

7	DOS Attack	CVE-2018-1000656	Python Flask vulnerability	The Pallets Project flask version Before 0.12.3 contains a CWE-20: Improper Input Validation vulnerability in flask that can result in Large amount of memory usage possibly leading to denial of service. This attack appear to be exploitable via Attacker provides JSON data in incorrect encoding. This vulnerability appears to have been fixed in 0.12.3. NOTE: this may overlap CVE-2019-1010083.	Protected by custom rules.	NA
		CVE-2021-28675	Pillow up to 8.1.x Data Block PSDImagePlugin.PsdImageFile denial of service	An issue was discovered in Pillow before 8.2.0. PSDImagePlugin.PsdImageFile lacked a sanity check on the number of input layers relative to the size of the data block. This could lead to a DoS on Image.open prior to Image.load.	Protected by custom rules.	NA
		CVE-2021-31807	Squid Web Proxy up to 4.14/5.0.5 HTTP Range Request denial of service	An issue was discovered in Squid before 4.15 and 5.x before 5.0.6. An integer overflow problem allows a remote server to achieve Denial of Service when delivering responses to HTTP Range requests. The issue trigger is a header that can be expected to exist in HTTP traffic without any malicious intent.	Protected by custom rules.	NA

8	External Entity Attack	CVE-2020-25817	SilverStripe up to 4.6.0-rc1 CSSContentParser xml external entity reference	SilverStripe through 4.6.0-rc1 has an XXE Vulnerability in CSSContentParser. A developer utility meant for parsing HTML within unit tests can be vulnerable to XML External Entity (XXE) attacks. When this developer utility is misused for purposes involving external or user submitted data in custom project code, it can lead to vulnerabilities such as XSS on HTML output rendered through this custom code. This is now mitigated by disabling external entities during parsing. (The correct CVE ID year is 2020 [CVE-2020-25817, not CVE-2021-25817]).	Protected by custom rules.	Detected by scanner as external entity attack.