Weekly Zero-Day Vulnerability Coverage Bulletin

December 2020

Total Zero Day Vulnerabilities found: 30

SQL Injection	Cross Site Scripting	Privilege Execution	Malicious File Upload	Command Injection	Remote Code Execution	OS Command Injection	DOS attack	Memory Corruption
4	18	1	1	1	2	1	1	1

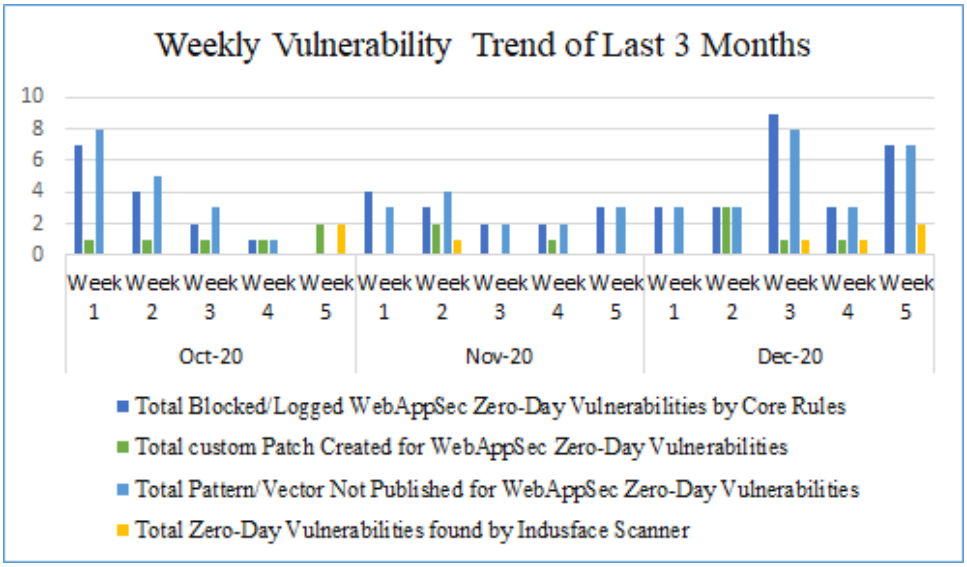
Zero-Day Vulnerabilities Protected through Core Rules	25
Zero-Day Vulnerabilities Protected through Custom Rules	5
Zero-Day Vulnerabilities for which protection cannot be determined	0 *
Zero-Day Vulnerabilities found by Indusface WAS	21 **

* 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:

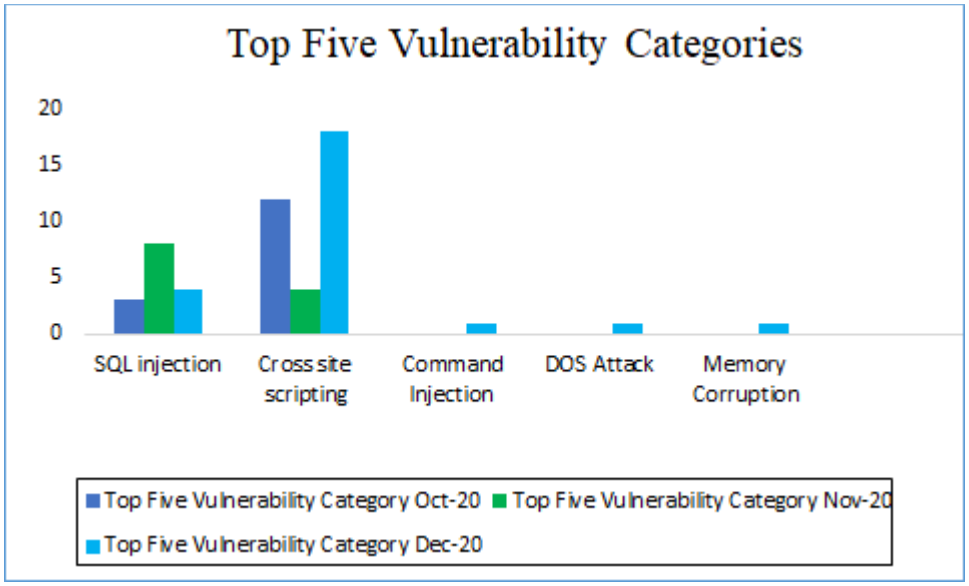
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



83% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

17% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

80% 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-2020-29283	Online Doctor Appointment Booking System getuser.php q sql injection	Online Doctor Appointment Booking System getuser.php q sql injection	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-20300	WeiPHP 5.0 wp_where sql injection	SQL injection vulnerability in the wp_where function in WeiPHP 5.0.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-35708	PHPList 3.5.9 Import Administrators Page sql injection	phpList 3.5.9 allows SQL injection by admins who provide a crafted fourth line of a file to the "Config - Import Administrators" page.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-35743	Hgiga MailSherlock URL Parameter sql injection [CVE-2020-35743]	A vulnerability, which was classified as critical, has been found inHgiga MailSherloc. This issue affects an unknown code of the componentURL Parameter Handle. There is no information	Protected by core rules.	Detected by scanner as SQL Injection attack.

				about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
2	Cross Site Scripting	CVE-2020-29572	MISP 2.4.135 genericField.ctp authkey comment cross site scripting	MISP 2.4.135 genericField.ctp authkey comment cross site scripting	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-7776	PHPOffice PhpSpreadsheet Excel File cross site scripting [CVE-2020-7776]	PHPOffice PhpSpreadsheet Excel File cross site scripting [CVE-2020-7776]	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-29455	SmartyStreets liveAddressPlugin.js 3.2 Parameter this.showInvalidCountry street/country cross site scripting	SmartyStreets liveAddressPlugin.js 3.2 Parameter this.showInvalidCountry street/country cross site scripting	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-35201	Ignite Realtime Openfire 4.6.0 create-bookmark.jsp users cross site scripting	Ignite Realtime Openfire 4.6.0 create-bookmark.jsp users cross site scripting	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-35121	Keysight Database Connector Plugin up to 1.4.x on Confluence Save Macro Parameter macro cross site scripting	An issue was discovered in the Keysight Database Connector plugin before 1.5.0 for Confluence. A malicious user could insert arbitrary JavaScript into saved macro parameters that would execute when a user viewed a page with that instance of the macro.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2020-28457	s-cart Package up to 4.3 Admin Dashboard AdminOrderController.phpindex cross site scripting	This affects the package s-cart/core before 4.4. The search functionality of the admin dashboard in core/src/Admin/Controllers/AdminOrderController.phpindex is vulnerable to XSS.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2019-14478	AdRem NetCrunch 10.6.0.4587 Web Client cross site scripting	Analysis Description. AdRem NetCrunch 10.6. 0.4587 has a stored Cross-Site Scripting (XSS) vulnerability in the NetCrunch web client. The user's input data is not properly encoded when being echoed back to the user.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-25611	Mitel MiCollab up to 9.1 AWV Portal cross site scripting	The AWV portal of Mitel MiCollab before 9.2 could allow an attacker to gain access to conference information by sending arbitrary code due to improper input validation, aka XSS. Successful exploitation could allow an attacker to view user conference information.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-12517	Phoenix Contact PLCnext prior 2021.0 LTS cross site scripting	On Phoenix Contact PLCnext Control Devices versions before 2021.0 LTS an authenticated low privileged user could embed malicious Javascript code to gain admin rights when the admin user visits the vulnerable website (local privilege escalation).	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2020-35475	MediaWiki up to 1.35.0 Raw HTML Special:UserRights cross site scripting	In MediaWiki before 1.35.1, the messages userrights-expiry-current and userrights-expiry-none can contain raw HTML. XSS can happen when a user visits Special:UserRights but does not have rights to change all userrights, and the table on the left side has unchangeable groups in it. (The right column with the changeable groups is not affected and is escaped correctly.)	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2020-26280	OpenSlides 3.2 cross site scripting [CVE-2020-26280]	OpenSlides is a free, Web-based presentation and assembly system for managing and projecting agenda, motions, and elections of assemblies. OpenSlides version 3.2, due to unsufficient user input validation and escaping, it is vulnerable to persistant cross-site scripting (XSS). In the web applications users can enter rich text in various places, e.g. for personal notes or in motions. These fields can be used to store arbitrary JavaScript Code that will be executed when other users read the respective text. An attacker could utilize this vulnerability be used to manipulate votes of other users, hijack the moderators session or simply disturb the meeting. The vulnerability was introduced with 6eae497abeab234418dfbd9d299e831eff86ed45 on 16.04.2020, which is first included in the 3.2 release. It has been patched in version 3.3	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	CVE-2019-9193	PgMiner botnet exploits disputed CVE to hack unsecured PostgreSQL DBs	PostgreSQL, also known as Postgres, is one of the most-used open-source relational database management systems (RDBMS) for production environments. It ranks fourth among all database management systems (DBMS) as of November 2020.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-35707	Daybyday 2.1.0 New Client Screen Name cross site scripting	Daybyday 2.1.0 allows stored XSS via the Company Name parameter to the New Client screen.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-26035	Zammad up to 3.4.0 Tags Element cross site scripting	An issue was discovered in Zammad before 3.4.1. There is Stored XSS via a Tags element in a TIcket.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	NA	DTLS Amplification Distributed Denial of Service Attack on Citrix ADC	To determine if a Citrix ADC or Citrix Gateway is being targeted by this attack, monitor the outbound traffic volume for any significant anomaly or spikes.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
	CVE-2020-29475	Nop Solution Ltd nopCommerce 4.30 Schedule Task Name cross site scripting	A vulnerability was found in Nop Solution Ltd nopCommerce 4.30. It has been classified as problematic. This affects an unknown function of the component Schedule Task Name Handler. 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 scanner as Cross Site Scripting attack.

	CVE-2020-5809	Umbraco CMS up to 8.9.1 TinyMCE Rich-Text Editor cross site scripting	A vulnerability was found in Umbraco CMS up to 8.9.1 and classified as problematic. This issue affects an unknown functionality of the component TinyMCE Rich-Text Editor. 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 scanner as Cross Site Scripting attack.
	CVE-2020-35740	Hgiga MailSherlock URL Parameter cross site scripting	A vulnerability was found in Hgiga MailSherlock. It has been rated as problematic. Affected by this issue is an unknown functionality of the component URL Parameter Handler. 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 scanner as Cross Site Scripting attack.

3	DOS Attack	NA	2FA bypass discovered in web hosting software cPanel	2FA bypass discovered in web hosting software cPanel	Protected by custom rules.	NA
4	Malicious File Upload	CVE-2020-28948, CVE-2020-28949	drupal-releases-out-band-security-updates-due-availability-exploits	Drupal Releases Out-of-Band Security Updates Due to Availability of Exploits	Protected by core rules.	Detected by scanner as Malicious file upload attack
5	Command injection	NA	Insecure Deserialization with JSON .NET	Serialization is the process of turning data objects into a stream of bytes that can be stored in files, memories, and databases or sent over a network, between different components of an application, and in API calls.	Protected by core rules.	Detected by scanner as Command Injection attack.
6	OS Command Injection Attack	NA	5 million WordPress sites potentially impacted by a Contact Form 7 flaw	“By exploiting this vulnerability, attackers could simply upload files of any type, bypassing all restrictions placed regarding the allowed upload-able file types on a website.” reads the post published by the Astra Security Research team. “Further, it allows an attacker to inject malicious content such as web shells into the sites that are using the Contact Form 7 plugin version below 5.3.1 and have file upload enabled on the forms.”	Protected by core rules.	Detected by Scanner as OS Command Injection Attack.
7	Privilege Escalation	CVE-2020-17530	Improper Control of Generation of Code ('Code Injection')	Apache Struts Possible Remote Code Execution vulnerability	Protected by custom rules.	NA

8	Memory Corruption	CVE-2020-4006	Russia-linked hackers actively exploit CVE-2020-4006 VMware flaw	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector address have a command injection vulnerability.	Protected by custom rules.	NA
9	Remote code execution	NA	Unauthenticated Command Injection bug opens D-Link VPN routers to hack	Security researchers at Digital Defense discovered three vulnerabilities in D-Link VPN routers, including command injection flaws, and an authenticated crontab injection flaw.	Protected by custom rules.	NA
		CVE-2020-35616	Joomla! Update Addresses Multiple Vulnerabilities	Joomla! Update Addresses Multiple Vulnerabilities	Protected by custom rules.	NA