Weekly Zero-Day Vulnerability Coverage Bulletin

(3rd February – 9th February)

Summary:

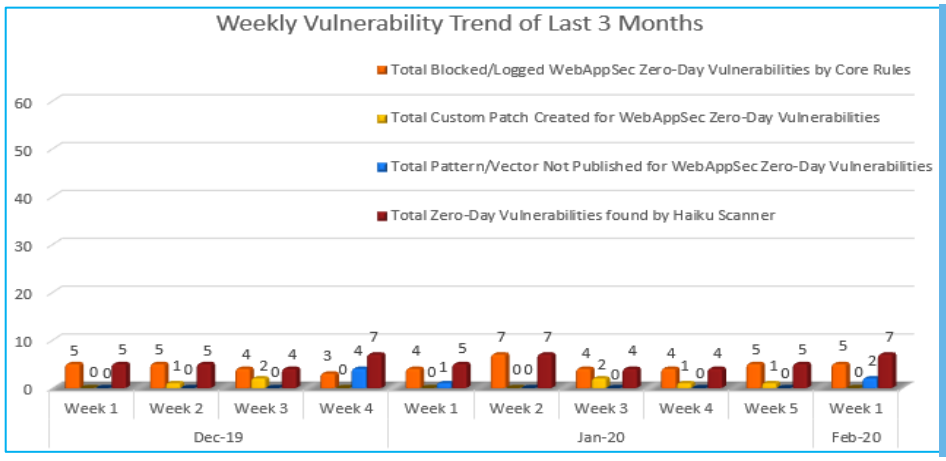
Total **7 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

2	3	1	1
Cross Site Scripting	SQL Injection	Brute Force	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	5
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	2**
Zero-Day Vulnerabilities found by Haiku Scanner	7

* 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:

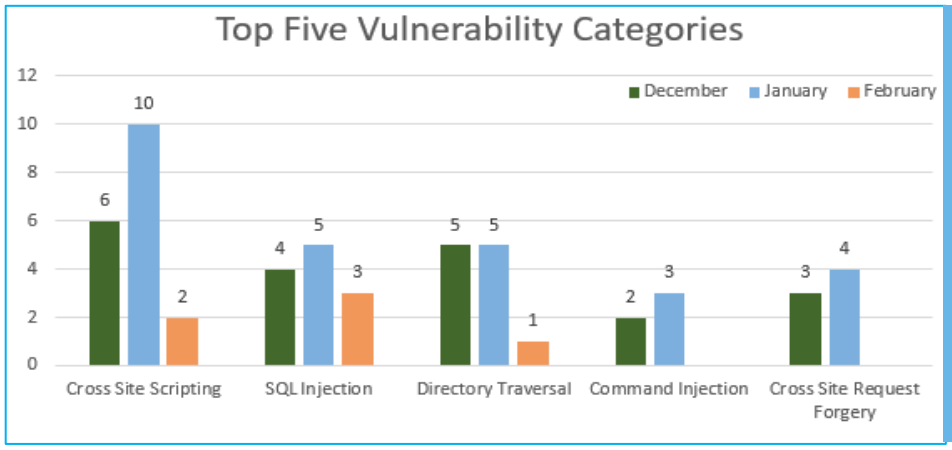


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

43% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

7% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

50% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting vulnerabilities are discovered in January compared to other months.

Zero Command Injection & Cross Site Request forgery attacks is discovered in February so far.

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.

Details:

S. No.	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Haiku Scanner Coverage
1.	Cross Site Scripting	NA	WordPress Plugin Bug Allows Malicious Code Injection on 100K Sites	Cross Site Scripting vulnerability in the popup-builder plugin before 3.64.1 for WordPress allows remote attackers to inject arbitrary JavaScript into existing popups via an unsecured ajax action in com/classes/Ajax.php. It is possible for an unauthenticated attacker to insert malicious JavaScript in several of the popup's fields by sending a request to wp-admin/admin-ajax.php with the POST action parameter of sgpb_autosave and including additional data in an allPopupData parameter, including the popup's ID (which is visible in the source of the page in which the popup is inserted) and arbitrary JavaScript which will then be executed in the browsers of visitors to that page. Because the plugin functionality automatically adds script tags to data entered these fields, this injection will typically bypass most WAF applications.	NA	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-3939	SysJust Syuan-Gu-Da-Shih cross site scripting [CVE-2020-3939]	A vulnerability was found in SysJust Syuan-Gu-Da-Shih and the affected version is unknown. It has been classified as problematic. This affects some unknown processing. Upgrading eliminates this vulnerability. A possible mitigation has been published before and not just after the disclosure of the vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2020-8592	eG Manager 7.1.2 Forgot Password com.eg.LoginHe	A vulnerability classified as critical was found in eG Manager 7.1.2. This vulnerability affects an	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

			lperServlet user sql injection	unknown code block of the file com.eg.LoginHelperServlet of the component Forgot Password. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2020-3937	SysJust Syuan-Gu-Da-Shih sql injection [CVE-2020-3937]	A vulnerability has been found in affected version unknown and classified as critical. Affected by this vulnerability is an unknown code. Upgrading eliminates this vulnerability. A possible mitigation has been published before and not just after the disclosure of the vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2019-20447	Jobberbase 2.0 jobs-in Endpoint PATH_INFO sql injection	A vulnerability, which was classified as critical, was found in Jobberbase 2.0. This affects an unknown function of the component jobs-in Endpoin. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	Brute Force	NA	WordPress Database Brute Force and Backdoors	WordPress login is not the only point of entry that hackers use to break into sites. Since the WordPress CMS stores most of its settings in a database, attackers can get access directly to the database to modify functionality and inject malicious code.	NA	Detected by scanner as Brute Force attack.
4.	Directory Traversal	CVE-2020-8545	AIL Framework 2.8 Global.py directory traversal	A vulnerability was found in AIL Framework 2.8 and classified as critical. This issue affects an unknown function of the file Global.py. There is no information about possible countermeasures known. It may be suggested to	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

	replace the affected object with an alternative product.