Weekly Zero-Day Vulnerability Coverage Bulletin

(18th March – 24th March)

Summary:

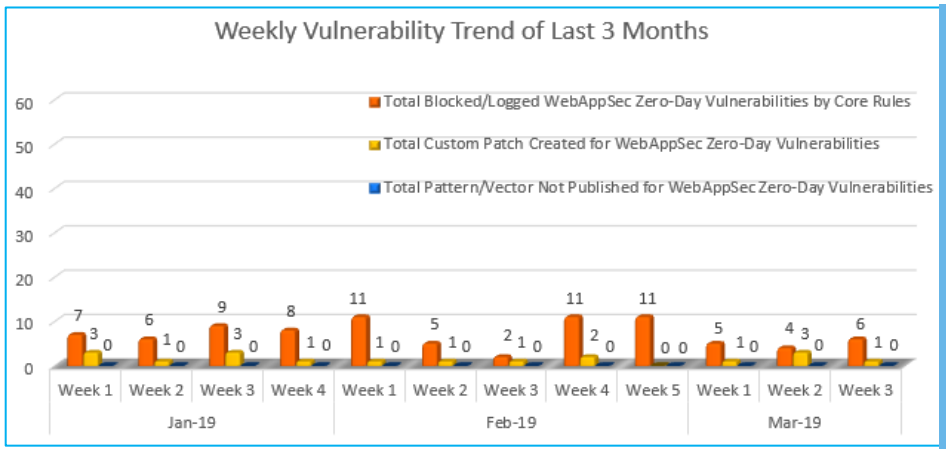
Total **7 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

3	1	2	1
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	6
Zero-Day Vulnerabilities Protected through Custom Rules	1*
Zero-Day Vulnerabilities for which protection cannot be determined	0**

* To enable custom rules please contact support@indusface.com
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

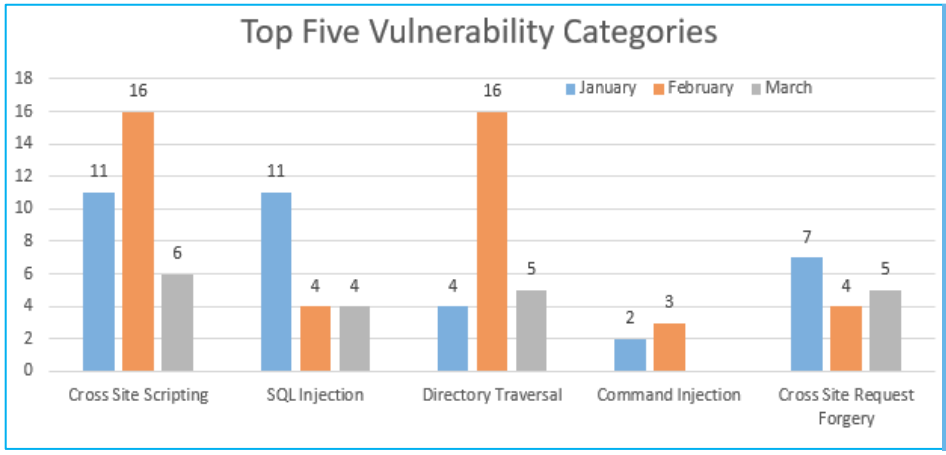
Vulnerability Trend:



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

84% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

16% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting vulnerabilities were discovered in December compared to other months and categories so far.

Medium no. of SQL Injection and CSRF attacks was found in all the months.

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
1.	Cross Site Scripting	CVE-2018-20806	Phamm 0.6.8 Login Page /public/main.php action cross site scripting	A vulnerability was found in Phamm 0.6.8. It has been classified as problematic. This affects code of the file */public/main.php* of the component *Login Page*. The manipulation of the argument action as part of a *Parameter* leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
		CVE-2018-1908	IBM 11 cross site scripting [CVE-2018-1908]	A vulnerability, which was classified as problematic, was found in IBM Robotic Process Automation with Automation Anywhere 11. This affects the function and manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance and would make it possible to initiate further attacks.	Protected by Default Rules.

		CVE-2016-5819	Moxa OnCell G3251 Reflected cross site scripting [CVE-2016-5819]	A vulnerability was found in Lenovo Dynamic Power Reduction Utility up to 2.2.1.x. It has been declared as critical. This vulnerability affects a code block of the component *Unquoted Search Path*. The manipulation with an unknown input leads to a privilege escalation vulnerability. The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published in 03/18/2019. The advisory is available at support.lenovo.com. This vulnerability was named as CVE-2019-6149.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-9083	SQLiteManager 1.2.0/1.2.4 main.php sql injection	A vulnerability was found in Lenovo Dynamic Power Reduction Utility up to 2.2.1.x. It has been declared as critical. This vulnerability affects a code block of the component *Unquoted Search Path*. The manipulation with an unknown input leads to a privilege escalation vulnerability. The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published 03/18/2019. The advisory is available at support.lenovo.com. This vulnerability was named as CVE-2019-6149.	Protected by Default Rules.

3.	Directory Traversal	CVE-2019-9618	GraceMedia Media Player Plugin up to 1.0 on WordPress ajax_controller. php cfg privilege escalation	A vulnerability was found in GraceMedia Media Player Plugin up to 1.0 on WordPress (Multimedia Player Software). It has been rated as critical. This issue affects some processing of the file */gracemedia-media-player/templates/files/ajax_controller.php*. The manipulation of the argument cfg with an unknown input leads to a privilege escalation vulnerability (Local File Inclusion). Using CWE to declare the problem leads to CWE-269. Impacted is confidentiality, integrity, and availability. The bug was discovered 02/06/2019. The weakness was released in 03/13/2019 by Manuel García Cárdenas	Protected by Default Rules.
		CVE-2019-9648	Core FTP Server 2.0 Build 674 SIZE Command directory traversal	A vulnerability was found in Lenovo Dynamic Power Reduction Utility up to 2.2.1.x. It has been declared as critical. This vulnerability affects a code block of the component *Unquoted Search Path*. The manipulation with an unknown input leads to a privilege escalation vulnerability. The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published in 03/18/2019. The advisory is available at support.lenovo.com. This vulnerability was named is CVE-2019-6149.	Protected by Default Rules.

4.	Cross Site Request Forgery	CVE-2019-1764	Cisco IP Phone 8800 Web-based Management Interface cross site request forgery	A vulnerability was found in Lenovo Dynamic Power Reduction Utility up to 2.2.1.x. It has been declared as critical. This vulnerability affects a code block of the component *Unquoted Search Path*. The manipulation with an unknown input leads to a privilege escalation vulnerability. The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published 03/18/2019. The advisory is available at support.lenovo.com. This vulnerability was named as CVE-2019-6149.	Protected by Custom Rules.