Weekly Zero-Day Vulnerability Coverage Bulletin

(15th April – 21st April)

Summary:

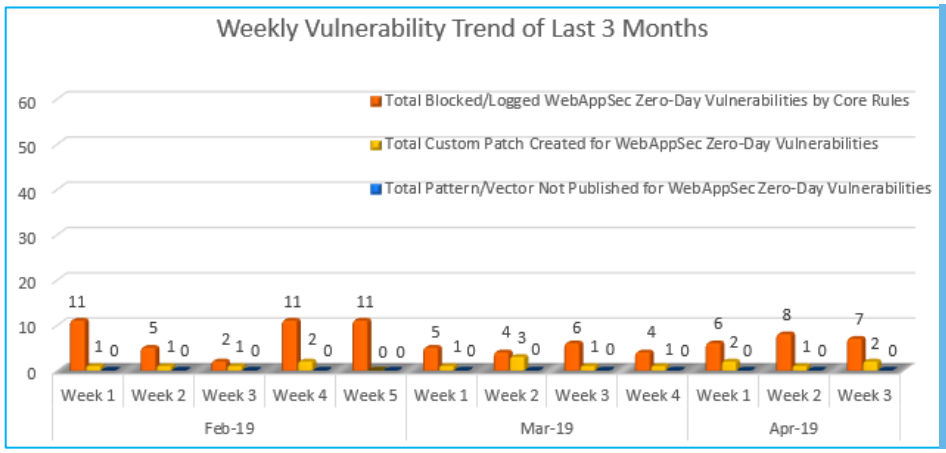
Total **9 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

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

Zero-Day Vulnerabilities Protected through Core Rules	7
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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

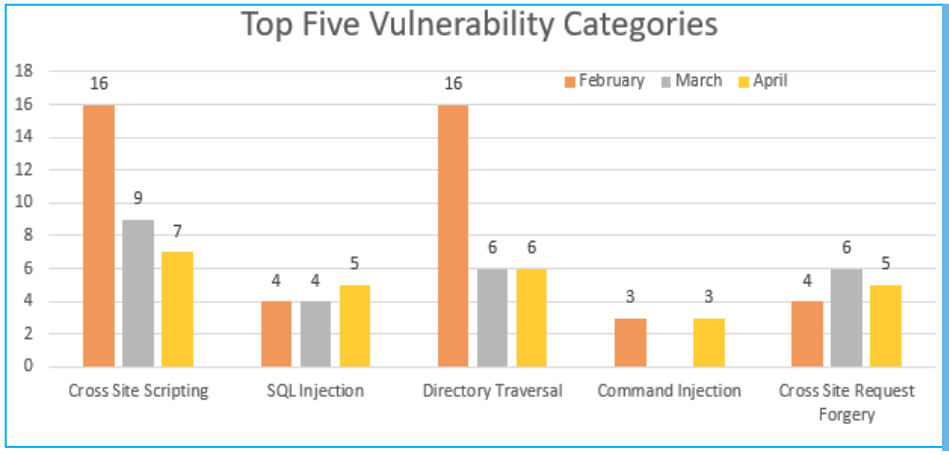
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

81% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

19% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



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

Medium no. of SQL Injection 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-2018-18261	Waimai Super CMS 20150505 addsave fcname cross site scripting	A vulnerability was found in Waimai Super CMS 20150505 (Content Management System) and classified as problematic. This issue affects a part of the file */admin.php/Foodcat/addsave*. The manipulation of the argument fcname as part of a *Parameter* leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-18019	Tribulant Slideshow Gallery Plugin 1.6.8 on WordPress admin.php Slide[title]/Slide[media_file]/Slide[image_url] cross site scripting	A vulnerability has been found in Tribulant Slideshow Gallery Plugin 1.6.8 on WordPress (Photo Gallery Software) and classified as problematic. This vulnerability affects a functionality of the file *wp-admin/admin.php?page=slideshow-slides&method=save*. The manipulation of the argument Slide[title]/Slide[media_file]/Slide[image_url] as part of a *Parameter* leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.

		CVE-2018-18017	Tribulant Slideshow Gallery Plugin 1.6.8 on WordPress admin.php Gallery[id]/Gallery[title] cross site scripting	A vulnerability, which was classified as problematic, has been found in Tribulant Slideshow Gallery Plugin 1.6.8 on WordPress (Photo Gallery Software). Affected by this issue is some functionality of the file *wp-admin/admin.php?page=slideshow-galleries&method=save*. The manipulation of the argument Gallery[id]/Gallery[title] as part of a *Parameter* leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-4012	IBM BigFix WebUI Profile Management Back-End Database sql injection	A vulnerability was found in IBM BigFix WebUI Profile Management and BigFix Software Distribution. It has been declared as critical. This vulnerability affects a code block of the component *Back-End Database*. The manipulation with an unknown input lead to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.

		CVE-2018-18018	Tribulant Slideshow Gallery Plugin 1.6.8 on WordPress admin.php Parameter sql injection	A vulnerability, which was classified as critical, was found in Tribulant Slideshow Gallery Plugin 1.6.8 on WordPress (Photo Gallery Software). This affects a function of the file *wp-admin/admin.php?page=slideshow-galleries&method=save*. The manipulation of the argument wp-admin/adminphp?page=slideshow-galleries&method=save as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-3396	Confluence Unauthorized RCE Vulnerability (CVE-2019-3396)	A vulnerability, which was classified as critical, has been found in Atlassian Confluence Server up to 6.6.11/6.12.2/6.13.2/6.14.1. Affected by this issue is some functionality of the component Widget Connector Macro. The manipulation with an unknown input leads to a directory traversal vulnerability (Code Execution). Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality, integrity, and availability.	Protected by Default Rules.
		CVE-2019-4178	IBM Cognos Analytics 11 URL Request directory traversal	A vulnerability was found in IBM Cognos Analytics 11 (Business Process Management Software). It has been	Protected by Default Rules.

				rated as critical. This issue affects some processing of the component *URL Handler*. The manipulation as part of a *Request* leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality, integrity, and availability. The weakness was published in 04/15/2019. It is possible to read the advisory at exchange.xforce.ibmcloud.com. The identification of this vulnerability is CVE-2019-4178 since 01/03/2019.	
4.	Cross Site Request Forgery	CVE-2019-10641	Contao 4.7 cross site request forgery [CVE-2019-10642]	A vulnerability classified as critical has been found in Contao 4.7. This affects an unknown function. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was published in 04/17/2019. The advisory is shared at contao.org.	Protected by Custom Rules.
		CVE-2019-3718	Dell SupportAssist Client up to 3.2 Origin Validator cross site request forgery	A vulnerability was found in Dell SupportAssist Client up to 3.2. It has been declared as problematic. This vulnerability affects a code block of the component *Origin	Protected by Custom Rules.

		Validator*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released in 04/18/2019.