Weekly Zero-Day Vulnerability Coverage Bulletin

(22nd April – 28th April)

Summary:

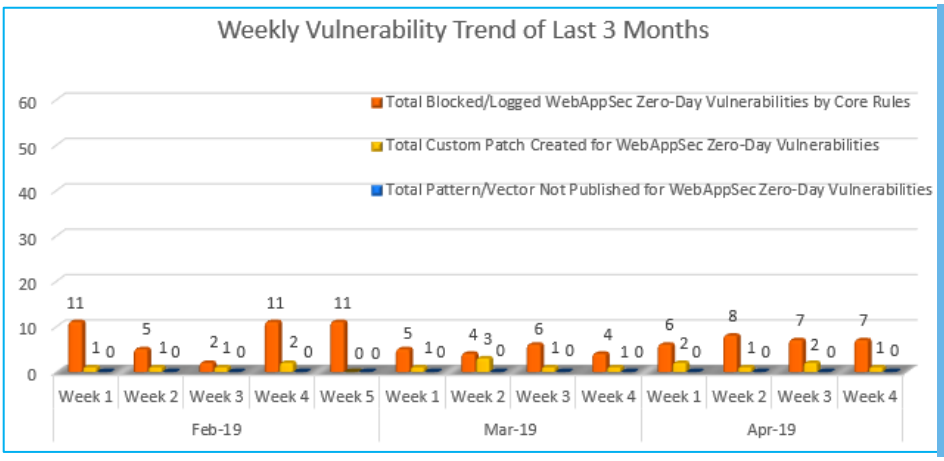
Total **9 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

3	3	1	2
Cross Site Scripting	SQL Injection	Remote Code Execution	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	8
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

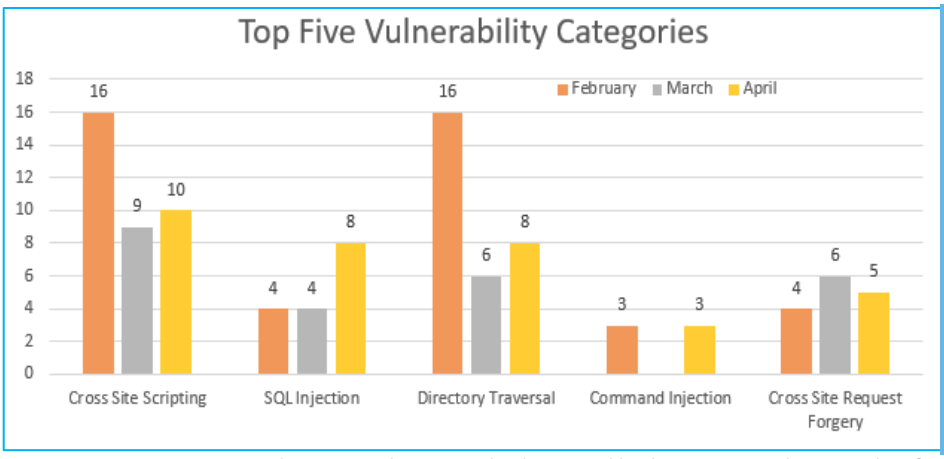
Vulnerability Trend:



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

82% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

18% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting and Directory Traversal vulnerabilities were discovered in February 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-2019-11449	I, Librarian 4.10 notes.php notes cross site scripting	A vulnerability classified as problematic has been found in I, Librarian 4.10. Affected is an unknown function of the file *notes.php*. The manipulation of the argument notes 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 web site. This would alter the appearance.	Protected by Default Rules.
		sa-core-2019-005 sa-core-2019-006 CVE-2019-10909	Drupal patched security vulnerabilities in Symfony, jQuery	The development team of the Symfony PHP web application framework released security updates for five issues, three of which also affects Drupal 7 and 8. The developers of the Symfony PHP web application framework addressed a total of five vulnerabilities, three of which impact the Drupal CMS. The flaws that affect the Drupal CMS are: 1) an arbitrary code flaw tracked as CVE-2019-10910; 2) the lack of a separator in the remember me cookie hash tracked as CVE-2019-10911; 3) a cross-site scripting (XSS) tracked as CVE-2019-10909.	Protected by Default Rules.
		CVE-2018-16219	AudioCodes 405HD 2.2.12 Web Interface cross site scripting	A vulnerability, which was classified as problematic, has been found in AudioCodes 405HD 2.2.12. This issue affects some functionality of the component *Web Interface*. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE	Protected by Default Rules.

				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. This would alter the appearance and would make it possible to initiate further attacks against.	
2.	SQL Injection	CVE-2019-11452	whatsns 4.0 cid[] sql injection	A vulnerability, which was classified as critical, was found in whatsns 4.0. This affects a function of the file *index.php?admin_category/remove.html*. The manipulation of the argument cid[] with an unknown input 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 inject and/or alter existing SQL statements which would influence the database exchange. The weakness was shared in 04/22/2019.	Protected by Default Rules.
		CVE-2019-11451	whatsns 4.0 qid sql injection	A vulnerability, which was classified as critical, has been found in whatsns 4.0. Affected by this issue is some functionality of the file *index.php?inform/add.html*. The manipulation of the argument qid with an unknown input lead to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was in 04/22/2019.	Protected by Default Rules.

		CVE-2019-11450	whatsns 4.0 title sql injection	A vulnerability classified as critical was found in whatsns 4.0. Affected by this vulnerability is the functionality of the file *index.php?question/ajax add.html*. The manipulation of the argument title 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 inject and/or alter existing SQL statements which would influence the database exchange. The weakness was disclosed in 04/22/2019.	Protected by Default Rules.
3.	Remote Code Execution	NA	ThinkPHP 5.x Remote Code Execution	A zero-day extensible markup language (XML) external entity (XXE) injection vulnerability in Microsoft Internet Explorer (IE) was recently disclosed by security researcher John Page. An attacker can reportedly exploit this vulnerability to steal confidential information or exfiltrate local files from the victim's machine. Page tested the vulnerability in the latest version of IE (11) with current patches on Windows 7 and 10, and Windows Server 2012 R2 operating systems. We looked at its attack chain to better understand how the security flaw works and how it can be mitigated.	Protected by Custom Rules.
4.	Directory Traversal	CVE-2019-7213	SmarterTools SmarterMail up to 16.x directory traversal	A vulnerability classified as critical was found in SmarterTools SmarterMail up to 16.x. Affected by this vulnerability is the functionality. The manipulation with an	Protected by Default Rules.

			unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was released 04/24/2019. It is possible to read the advisory at smartertools.com. This vulnerability is known as CVE-2019-7213 since 01/29/2019.	
	CVE-2019-3720	Dell EMC Open Manage System Administrator up to 9.2.x directory traversal	A vulnerability was found in Dell EMC Open Manage System Administrator up to 9.2.x. It has been declared as critical. Affected by this vulnerability is a code block. The manipulation with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was disclosed 04/25/2019. This vulnerability is known as CVE-2019-3720 since 01/03/2019. The attack can be launched remotely.	Protected by Default Rules.