Weekly Zero-Day Vulnerability Coverage Bulletin

(6th May – 12th May)

Summary:

Total **8 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

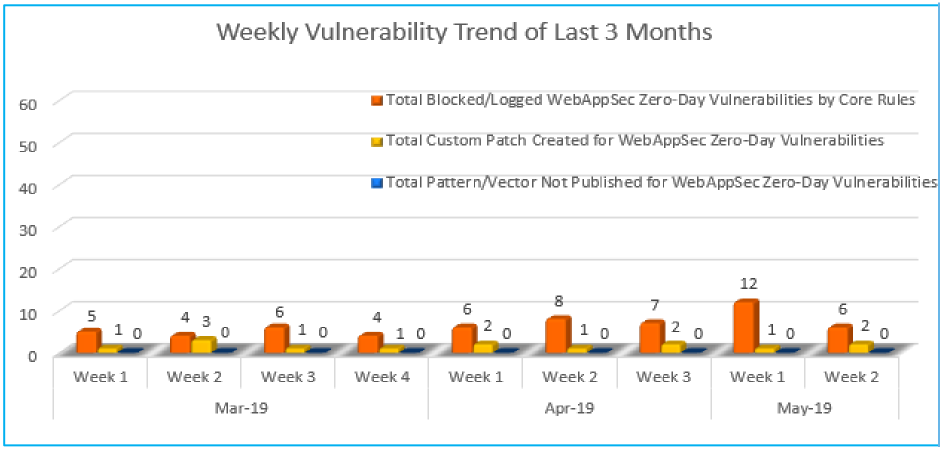
3	**1**	**2**	**2**
Cross Site Scripting	Command Injection	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	6
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

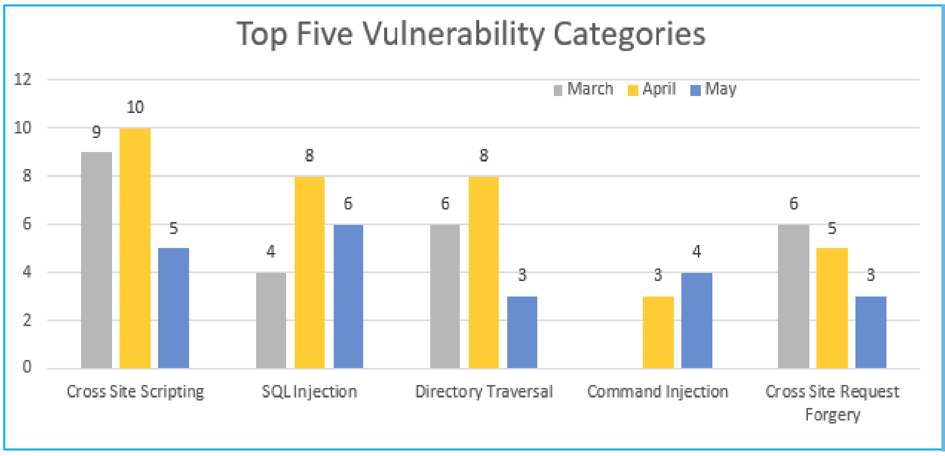
Vulnerability Trend:



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

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, SQL Injection & Directory Traversal vulnerabilities were discovered in April compared to other months and categories so far.

Zero Command Injection vulnerabilities are found in March.

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-2018-4065	Sierra Wireless AirLink ES450 4.9.3 ACEManager ping_result.cgi cross site scripting	A vulnerability classified as problematic was found in Sierra Wireless AirLink ES450 4.9.3. Affected by this vulnerability is the functionality of the file *ping_result.cgi* of the component *ACEManager*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Reflected). 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. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-11406	Subrion CMS 4.2.1 _core/en/contacts/ name/email/phone cross site scripting	A vulnerability was found in Subrion CMS 4.2.1 (Content Management System). It has been rated as problematic. This issue affects some processing of the file *_core/en/contacts/*. The manipulation of the argument name/email/phone 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. This would alter the appearance.	Protected by Default Rules.

		CVE-2019-11398	UliCMS 2019.1/2019.2 admin/index.php go cross site scripting	A vulnerability was found in UliCMS 2019.1/2019.2. It has been declared as problematic. This vulnerability affects a code block of the file *admin/index.php*. The manipulation of the argument goes 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.
2.	Command Injection	CVE-2018-4061	Sierra Wireless AirLink ES450 4.9.3 ACEManager iplogging.cgi HTTP Request command injection	A vulnerability was found in Sierra Wireless AirLink ES450 4.9.3. It has been declared as critical. This vulnerability affects a code block of the file *iplogging.cgi* of the component *ACEManager*. The manipulation as part of a *HTTP Request* leads to a privilege escalation vulnerability (Command Injection). The CWE definition for the vulnerability is CWE-88. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was disclosed in 05/06/2019. This vulnerability was named CVE-2018-4061 since 01/02/2018.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-6617	F5 BIG-IP up to 11.5.8/11.6.3.4/12.1.4/13.1.1.4/14.1.0.1 sftp directory traversal	A vulnerability was found in F5 BIG-IP up to 11.5.8/11.6.3.4/12.1.4/13.1.1.4/14.1.0.1 (Firewall Software) and classified as critical. Affected by this issue is a part of the component *sftp*. The manipulation with an	Protected by Default Rules.

				unknown input leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. The weakness was shared in 05/03/2019. The advisory is shared for download at support.f5.com. This vulnerability is handled as CVE-2019-6617 since 01/22/2019.	
		CVE-2019-6614	F5 BIG-IP up to 12.1.4/13.1.1.4/ 14.1.0.1 Appliance Mode directory traversal	A vulnerability, which was classified as critical, has been found in F5 BIG-IP up to 12.1.4/13.1.1.4/14.1.0.1 (Firewall Software). This issue affects some functionality of the component *Appliance Mode*. The manipulation with an unknown input 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 released in 05/03/2019. The advisory is shared at support.f5.com. The identification of this vulnerability is CVE-2019-6614 since 01/22/2019.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2019-5430	UniFi Video up to 3.10.0 Web API cross site request forgery	A vulnerability classified as problematic was found in UniFi Video up to 3.10.0. This vulnerability affects the functionality of the component *Web API*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-	Protected by Custom Rules.

			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 presented in 05/06/2019. This vulnerability was named as CVE-2019-5430	
	CVE-2018-4066	Sierra Wireless AirLink ES450 up to 4.9.3 ACEManager HTTP Request cross site request forgery	A vulnerability, which was classified as problematic, has been found in Sierra Wireless AirLink ES450 up to 4.9.3. Affected by this issue is some functionality of the component *ACEManager*. The manipulation as part of a *HTTP Request* leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was released in 05/06/2019.	Protected by Custom Rules.