Weekly Zero-Day Vulnerability Coverage Bulletin

(26th November – 2nd December)

Summary:

Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** in this week

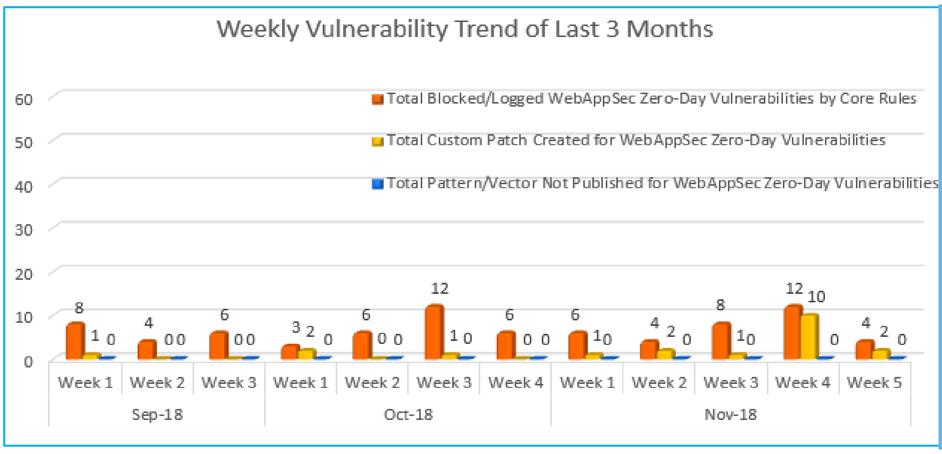
3 Cross Site Scripting	**2** Cross Site Request Forgery	**1** Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	4
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

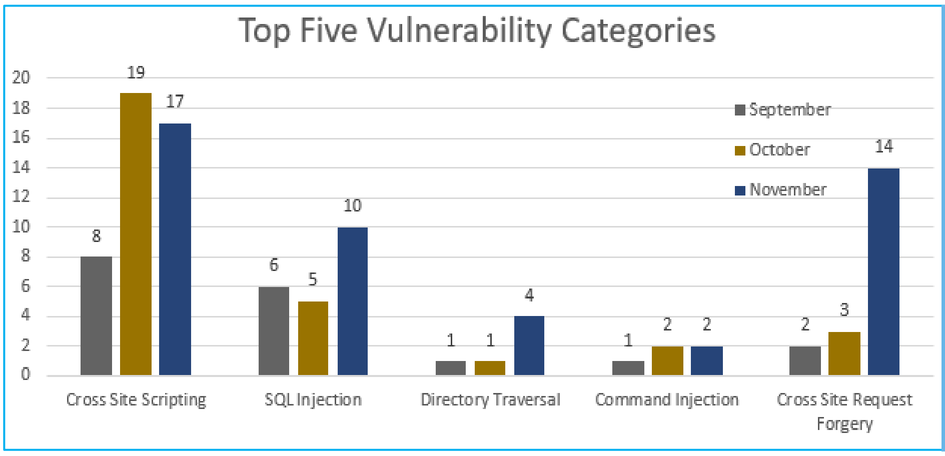
Vulnerability Trend:



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

80% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

20% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum no. of Cross Site Scripting vulnerabilities were discovered in October compared to other months and categories so far.

Medium no. of SQL Injection 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-2018-19564	Easy Testimonials Plugin 3.2 on WordPress wp-admin/post.php _ikcf_client/_ikcf_position/_ikcf_other cross site scripting	A vulnerability was found in Easy Testimonials Plugin 3.2 on WordPress. It has been classified as problematic. This affects an unknown function of the file *wp-admin/post.php*. The manipulation of the argument _ikcf_client/_ikcf_position/_ikcf_other as part of a *Parameter* leads to a cross site scripting vulnerability (Stored). 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-2018-13312	TOTOLINK A3002RU 1.0.8 notice_gen.htm cross site scripting	A vulnerability was found in TOTOLINK A3002RU 1.0.8. It has been rated as problematic. This issue affects an unknown function of the file *notice_gen.htm*. The manipulation with an unknown input 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 web site. This would alter the appearance and would possibly initiate further attacks against.	Protected by Default Rules.
		CVE-2018-13310	TOTOLINK A3002RU 1.0.8 password.htm Username cross site scripting	A vulnerability was found in TOTOLINK A3002RU 1.0.8. It has been classified as problematic. This affects an unknown function of the file *password.htm*. The manipulation as part of a *Username* 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	Protected by Default Rules.

				might be able to inject arbitrary html and script code into the web site. This would alter the appearance.	
2.	Cross Site Request Forgery	CVE-2018-19561	sikcms 1.1 admin.php cross site request forgery	A vulnerability has been found in sikcms 1.1 and classified as problematic. Affected by this vulnerability is an unknown function of the file *admin.php?m=Admin&c=Users&a=userAdd*. 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 disclosed in 11/26/2018. This is a known vulnerability.	Protected by Custom Rules.
		CVE-2018-19544	JEECMS 9.3 api/admin/content/save cross site request forgery	A vulnerability was found in JEECMS 9.3 and classified as problematic. Affected by this issue is an unknown function of the file *api/admin/content/save*. The manipulation with an unknown input 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 force legitimate users to initiate unwanted actions within the web application. The weakness was published 11/26/2018. This vulnerability is handled as CVE-2018-19544 since 11/25/2018.	Protected by Custom Rules.

3.	Command Injection	CVE-2018-19646	Imperva SecureSphere 13.0.10/13.1.10 /13.2.10 Python CGI Script Argument command injection	A vulnerability has been found in Imperva SecureSphere 13.0.10/13.1.10/13.2.10 and classified as critical. This vulnerability affects an unknown function of the component *Python CGI Script*. The manipulation as part of a *Argument* 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 11/28/2018 as *EDB-ID 45542* as uncorroborated exploit (Exploit-DB). The advisory is available at exploit-db.com.	Protected by Default Rules.