Weekly Zero-Day Vulnerability Coverage Bulletin

(18th November – 24th November)

Summary:

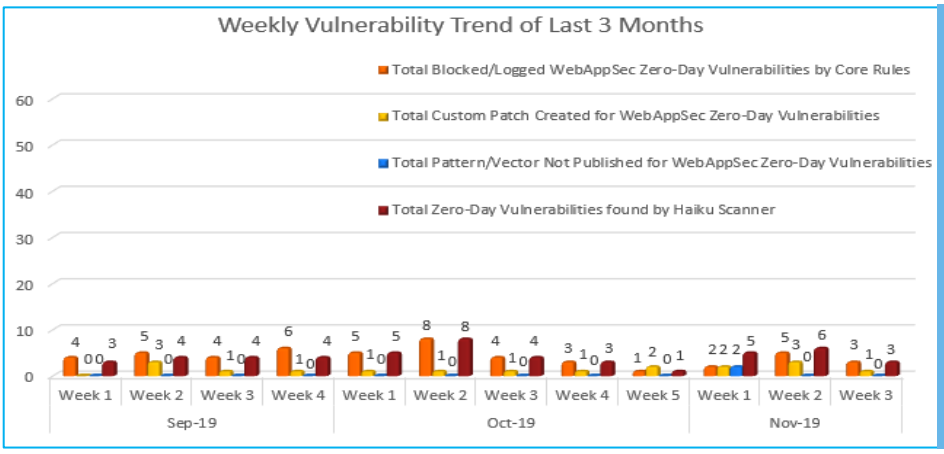
Total **4 Zero-Day Vulnerabilities** were discovered in **3 Categories** in this week

2	1	1
Cross Site Scripting	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	3
Zero-Day Vulnerabilities Protected through Custom Rules	1*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	3

* 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:

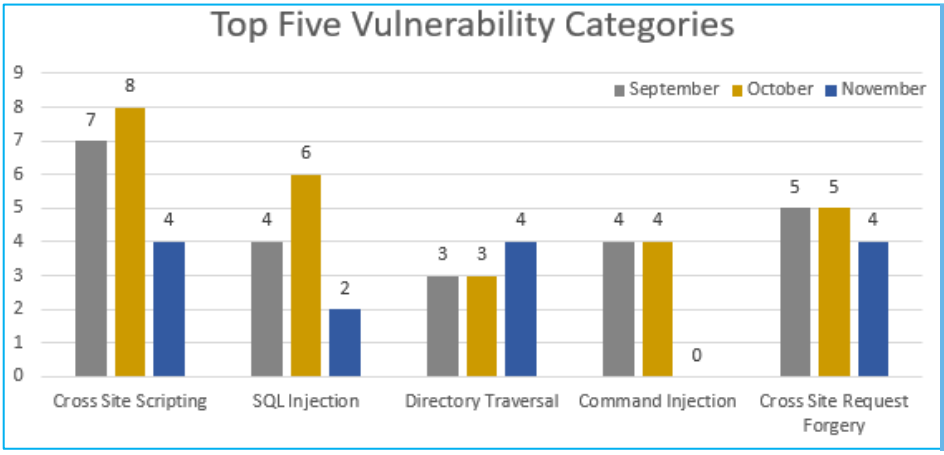


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

42% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

14% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

42% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting vulnerabilities are discovered in October compared to other months.

Zero Command Injection is discovered in November so far.

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	Haiku Scanner Coverage
1.	Cross Site Scripting	NA	High Severity Vulnerability Patched in WP Maintenance Plugin	WP Maintenance, a WordPress plugin with approximately 30,000+ active installs. This flaw could allow attackers to enable a vulnerable site's maintenance mode and inject malicious code affecting site visitors. Plugin versions of WP Maintenance up to 5.0.5 are vulnerable to attacks against this flaw.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2012-4439	Jenkins up to 1.481/LTS 1.466.1 URL cross site scripting	A vulnerability was found in Jenkins up to 1.481/LTS 1.466.1 (Continuous Integration Software). It has been classified as problematic. This affects an unknown code of the component URL Handler. Upgrading to version 1.482 or LTS 1.466.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Directory Traversal	CVE-2019-10765	iobroker.admin up to 3.6.11 Local File Inclusion [CVE-2019-10765]	A vulnerability, which was classified as problematic, has been found in iobroker.admin up to 3.6.11. Affected by this issue is an unknown functionality. Upgrading to version 3.6.12 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
3.	Cross Site Request Forgery	CVE-2012-2079	Activity Module 6.x-1.x on Drupal cross site request forgery	A vulnerability classified as problematic was found in Activity Module 6.x-1.x on Drupal.	Protected by Custom Rules.	NA

	Affected by this vulnerability is an unknown code. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.