Weekly Zero-Day Vulnerability Coverage Bulletin

(28th October – 3rd November)

Summary:

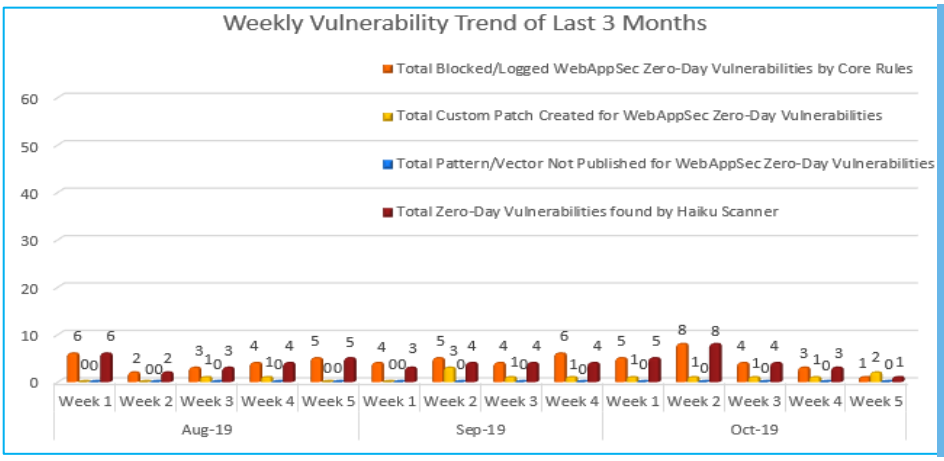
Total **3 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

1	1	1
Cross Site Scripting	Cross Site Request Forgery	Malicious File Upload

Zero-Day Vulnerabilities Protected through Core Rules	1
Zero-Day Vulnerabilities Protected through Custom Rules	2*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	1

* 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:

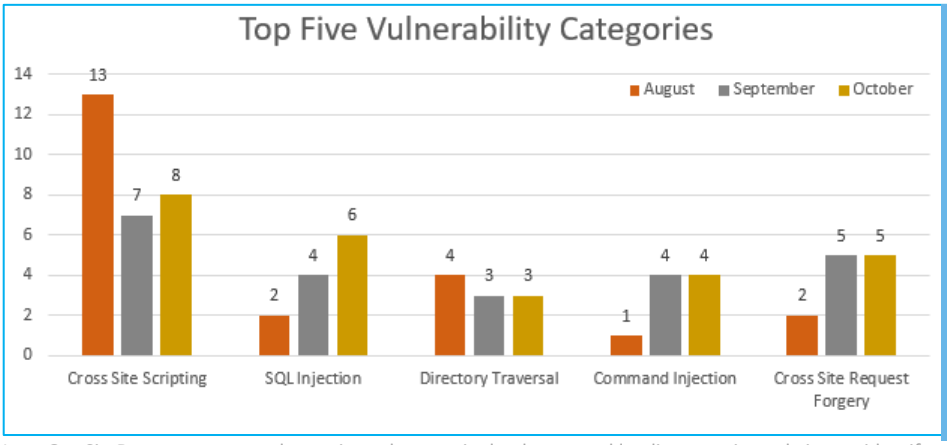


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

46% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

11% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

43% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum no. of Cross Site Scripting vulnerabilities are discovered in August compared to other months.

Only 1 Command Injection attack was discovered in August compared to other months and categories.

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	Zero Day Vulnerability in Rich Reviews Plugin Exploited in the Wild	The estimated 16,000 sites running the plugin are vulnerable to unauthenticated plugin option updates, which can be used to deliver stored cross-site scripting (XSS) payloads. Attackers are currently abusing this exploit chain to inject malvertising code into target websites. The malvertising code creates redirects and popup ads.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Cross Site Request Forgery	NA	Tiki Wiki CMS Groupware 5.2 tiki-adminusers.php cross site request forgery	A vulnerability was found in Tiki Wiki CMS Groupware 5.2 (Groupware Software). It has been rated as problematic. Affected by this issue is an unknown function of the file tiki-adminusers.php. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA
3.	Malicious File Upload	NA	Web Shells Penetration Testing	A web-shell is a malicious script used by an attacker with the intent to escalate and maintain persistent access on an already compromised web application. Web-shells cannot attack or exploit a remote vulnerability, so it is always the second step of an attack (this stage is also referred to as post-exploitation). An attacker can take advantage of common vulnerabilities such as SQL injection, remote file inclusion (RFI), FTP, or even use cross-site scripting (XSS) as part of a social engineering attack in order to upload the malicious script. The common functionality is included but is not limited to shell command execution, code execution, database enumeration and file management.	Protected by Custom Rules.	NA