Weekly Zero-Day Vulnerability Coverage Bulletin

(23rd September – 29th September)

Summary:

Total **7 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

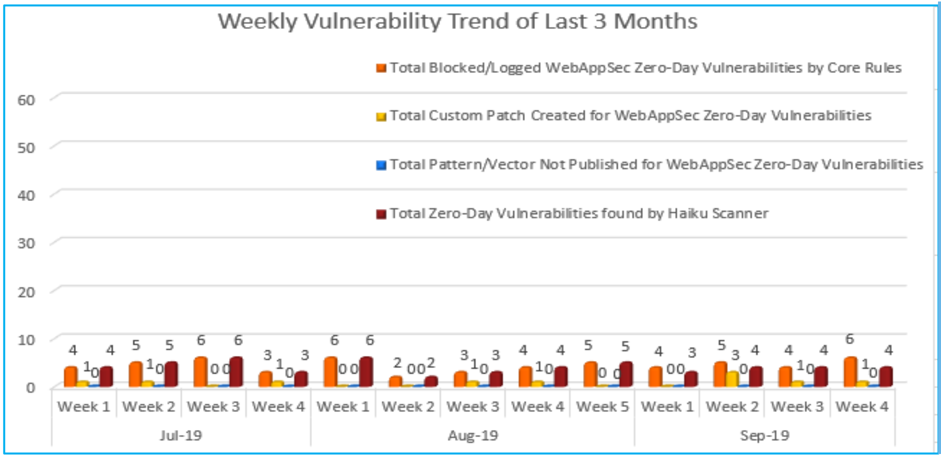
2	**2**	**1**	**1**	**1**
Cross Site Scripting	SQL Injection	Host Header Injection	Cross Site Request Forgery	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	6
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	4

* 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:

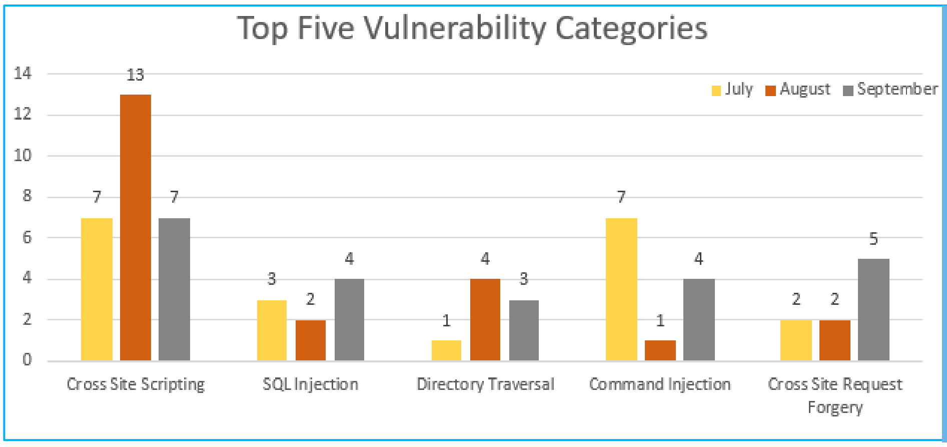


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

48% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

8% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

44% 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 August compared to other months.

Only 1 Command Injection attack is discovered in August and 1 Directory Traversal in July.

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	Attackers are currently abusing this xss exploit chain to inject malvertising code into target websites. The malvertising code creates redirects and popup ads. Two core issues in the Rich Reviews plugin are a lack of access controls for modifying the plugin's options, and a subsequent lack of sanitization on the values of those options.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Anonymous researcher drops vBulletin zero-day impacting tens of thousands of sites	vBulletin 5.x through 5.5.4 allows remote command execution via the widgetConfig[code] parameter in an ajax/render/widget_php routestring request.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-16696	phpipam 1.4 edit.php table sql injection	A vulnerability, which was classified as critical, has been found in <a href="https://vuldb.com/?product.phpipam">phpipam 1.4</a>. Affected by this issue is an unknown code block of the file <em>app/admin/custom-fields/edit.php</em>. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	NA
		CVE-2019-16694	phpipam 1.4 edit-result.php table sql injection	A vulnerability classified as critical has been found in <a href="https://vuldb.com/?product.phpipam">phpipam 1.4</a>. Affected is an unknown part of the file <em>app/admin/custom-fields/edit-result.php</em>. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	NA
3.	Host Header Injection	CVE-2019-16532	YzmCMS 5.3 HTTP Host Header Open Redirect	A vulnerability classified as critical has been found in <a href="https://vuldb.com/?product.yzmcms">YzmCMS 5.3</a>. This affects an unknown code of the component <em>HTTP Host Header Handler</em>. There is no information about possible countermeasures known. It may be	Protected by Default Rules.	Detected by scanner as Host Header Injection attack.

				suggested to replace the affected object with an alternative product.		
4.	Cross Site Request Forgery	CVE-2019-16721	NoneCms 1.3 dele.html cross site request forgery	A vulnerability was found in <a href="https://vuldb.com/?product.nonecms">NoneCms 1.3</a>. It has been declared as problematic. Affected by this vulnerability is an unknown function of the file <em>public/index.php/admin/admin/dele.html</em>. 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
5.	Directory Traversal	CVE-2019-16867	HongCMS 3.0.0 ajax file directory traversal	A vulnerability, which was classified as problematic, has been found in <a href="https://vuldb.com/?product.hongcms">HongCMS 3.0.0</a>. Affected by this issue is an unknown function of the file <em>admin/index.php/database/ajax?action=delete</em>. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.