Weekly Zero-Day Vulnerability Coverage Bulletin

(16th September – 22nd September)

Summary:

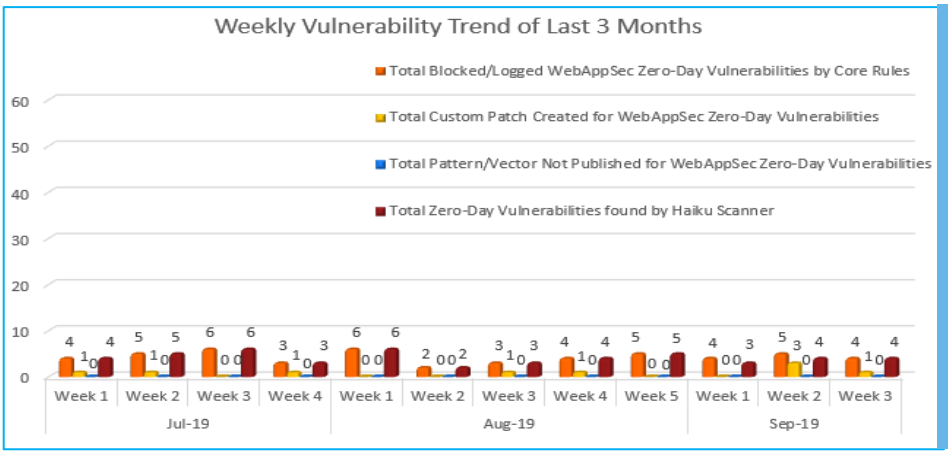
Total **5 Zero-Day Vulnerabilities** were discovered in **3 Categories** in this week

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

Zero-Day Vulnerabilities Protected through Core Rules	4
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:

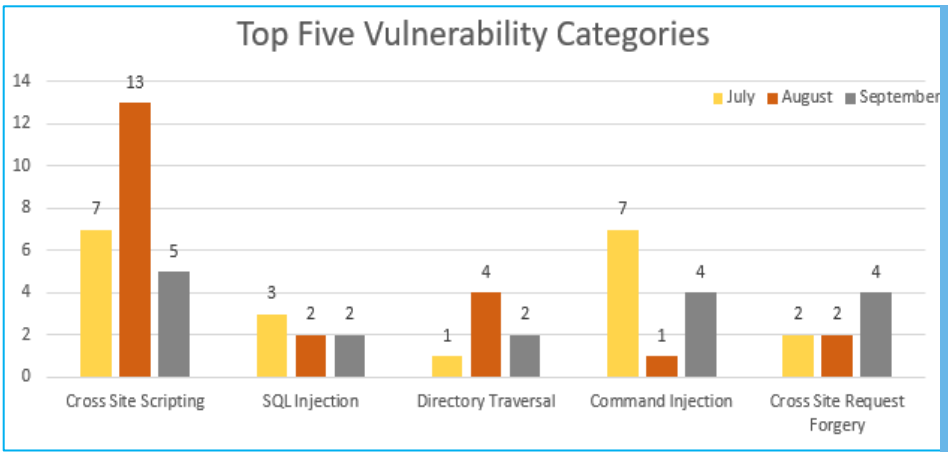


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

47% 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

45% 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	CVE-2016-10963	icegram Plugin up to 1.9.18 on WordPress cross site scripting	A vulnerability has been found in icegram Plugin up to 1.9.18 on WordPress (WordPress Plugin) and classified as problematic. Affected by this vulnerability is an unknown code. Upgrading to version 1.9.19 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	WordPress XSS Bug Allows Drive-By Code Execution	The bug exists in the built-in editor Gutenberg which fails to filter a post's JavaScript/HTML code if there's a "Shortcode" error message. Shortcodes are essentially shortcuts that WordPress users can utilize to embed files or create objects that would normally require more complex code to accomplish. Shortcode blocks can be added to a page by clicking on the "Add Block button" inside the Gutenberg editor.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Command Injection	CVE-2019-15846	CVE-2019-15846 Privileged Remote Code Execution Vulnerability in the Exim Mailer: What You Need to Know	An unauthenticated remote attacker could send a malicious SNI ending in a backslash-null sequence during the initial TLS handshake, which causes a buffer overflow in the SMTP delivery process. This would allow an attacker to inject malicious code that Exit then arbitrarily executes as root. This vulnerability does not depend on the TLS library in use, so both	Protected by Default Rules.	Detected by scanner as Command Injection attack.

				GnuTLS and OpenSSL are affected.		
		CVE-2017-9841	Drupal Sites Exploited Using PHPUnit Vulnerability in Mailchimp Modules (PSA-2019-0904)	There is a vulnerability in PHPUnit, a widely used testing framework for PHP. The vulnerability can lead to remote code execution (RCE). Usually phpunit is deployed using composer, a very popular dependency manager for PHP. In most cases phpunit isn't required for the production environment, but nonetheless it is installed. Placing composer modules into web accessible directory is another common mistake that allows direct exploitation of this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
3.	Cross Site Request Forgery	NA	Researcher Drops phpMyAdmin Zero-Day Affecting All Versions	This has been detected as Cross-Site Request Forgery in phpMyAdmin, that allows an attacker to trigger a CSRF attack against a phpMyAdmin user deleting any server in the Setup page.	Protected by Custom Rules.	NA