Weekly Zero-Day Vulnerability Coverage Bulletin

(23rd July – 29th July)

Summary:

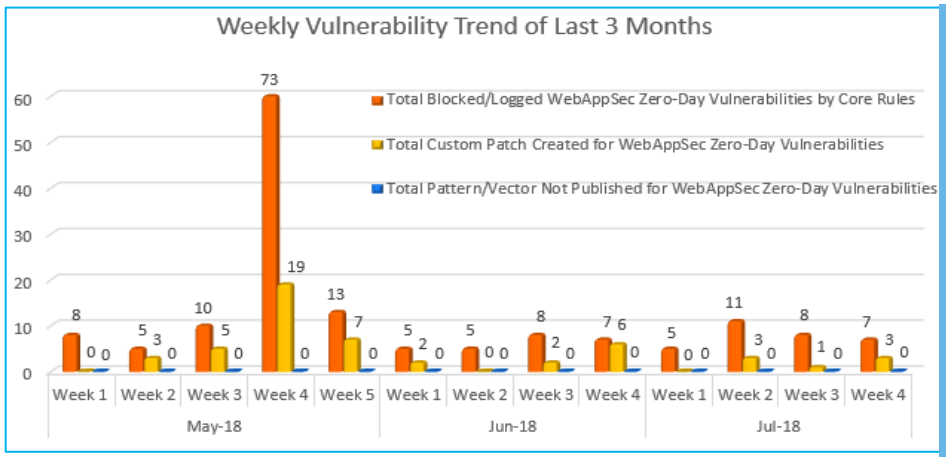
Total **10 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

3	3	3	1
Cross Site Scripting	Local File Inclusion	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	7
Zero-Day Vulnerabilities Protected through Custom Rules	3*
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:

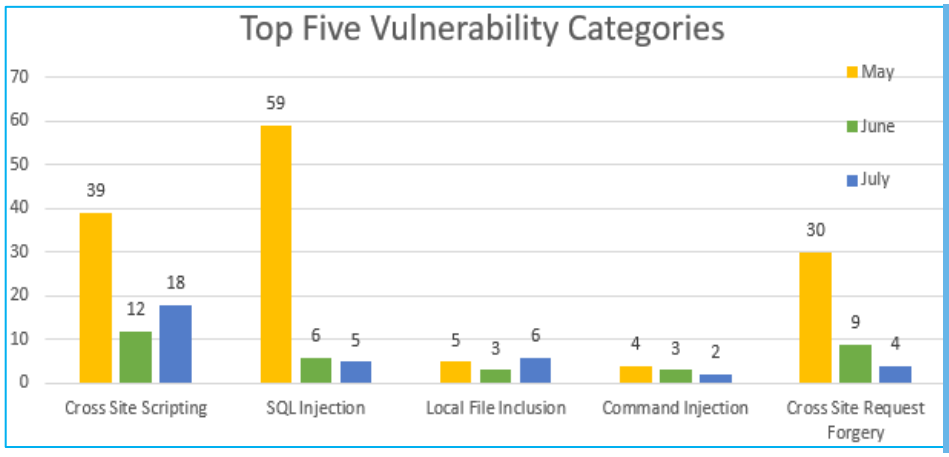


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

May 4th Week has multiple vulnerabilities blocked by Core Rules.

76% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

24% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that multiple SQL Injection vulnerabilities were discovered in May compared to other months and categories.

Medium no. of Cross Site Scripting attacks was found in May compared to June.

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	EDB-ID: 148651	Linksys.com Cross Site Scripting	Linksys.com suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 148665	McAfee.com Redirect Cross Site Scripting	A URL redirect at mcafee.com suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 45084	D-link DAP-1360 - Path Traversal / Cross-Site Scripting	After Successfully Connected to D-Link DIR-600 Router(FirmWare Version : 2.01), Any User Can Bypass The Router's Root password as well bypass admin panel.	Protected by Default Rules.
2.	Local File Inclusion	CVE-2018-0296	Cisco Adaptive Security Appliance Path Traversal	This Metasploit module exploits a security vulnerability in Cisco ASA that would allow an attacker to view sensitive system information without authentication by using directory traversal techniques.	Protected by Default Rules.
		EDB-ID: 148670	GeoVision GV-SNVR0811 Directory Traversal	GeoVision GV-SNVR0811 suffers from a directory traversal vulnerability.	Protected by Default Rules.
		EDB-ID: 45065	GeoVision GV-SNVR0811 - Directory Traversal	GeoVision GV-SNVR0811 - Directory Traversal	Protected by Default Rules.
3.	Cross Site Request Forgery	CVE-2015-5996	Tenda Wireless N150 Router 5.07.50 Cross Site Request Forgery	Tenda Wireless N150 Router version 5.07.50 suffers from a cross site request forgery vulnerability.	Protected by Custom Rules.
		EDB-ID: 148664	Shopclues.com Cross Site Request Forgery	Shopclues.com suffers from a cross site request forgery vulnerability.	Protected by Custom Rules.
		CVE-2018-13859	Trivum Multiroom Setup Tool 8.76 Cross Site Request Forgery	Trivum Multiroom Setup Tool version 8.76 suffers from a cross site request forgery vulnerability.	Protected by Custom Rules.
4.	Command Injection	EDB-ID: 148669	NUUO NVRmini upgrade_handle.php Remote Command Execution	NUUO NVRmini suffers from a remote command execution vulnerability in upgrade_handle.php.	Protected by Default Rules.