Weekly Zero-Day Vulnerability Coverage Bulletin

(30th July – 5th August)

Summary:

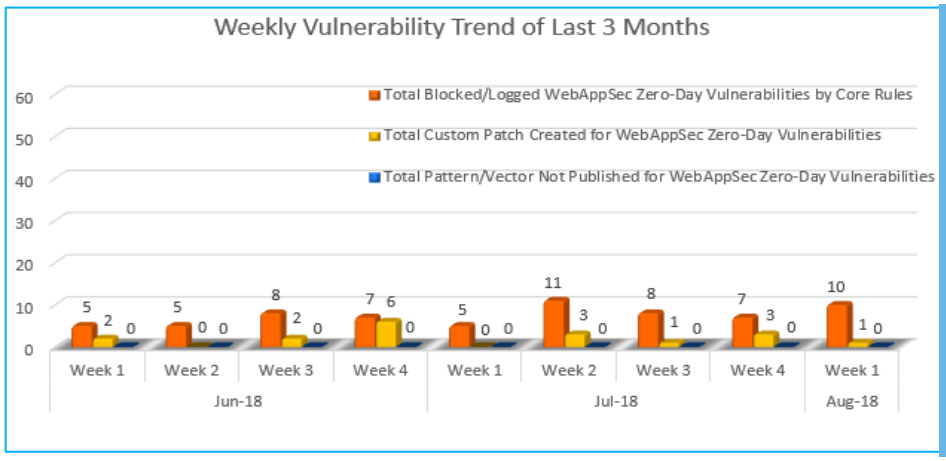
Total **11 Zero-Day Vulnerabilities** were discovered in **5 Categories** previous week

5	2	2	1	1
Cross Site Scripting	SQL Injection	Local File Inclusion	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	10
Zero-Day Vulnerabilities Protected through Custom Rules	1*
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

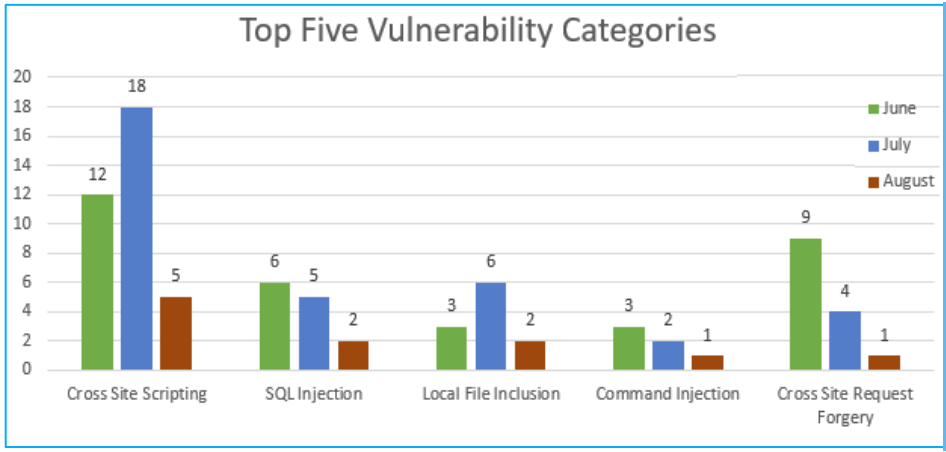
Vulnerability Trend:



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

77% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

23% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting vulnerabilities were discovered in July compared to other months and categories so far.

Medium no. of SQL Injection attacks was found in all the months.

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	CVE-2018-13256	Chartered Accountant: Auditor Website 2.0.1 Cross Site Scripting	Chartered Accountant: Auditor Website version 2.0.1 suffers from a Cross site scripting vulnerability.	Protected by Default Rules.
		CVE-2018-14541	PHP Scripts Mall Basic B2B Script 2.0.0 First Name/Last Name/Address 1/city/state/ company reflected Cross Site Scripting	A vulnerability has been found in PHP Scripts Mall Basic B2B Script 2.0.0 and classified as problematic. This vulnerability affects an unknown function. The manipulation of the argument First name/Last name/Address 1/City/State/Company wit h an unknown input leads to a cross site scripting vulnerability (Reflected). The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by Default Rules.
		CVE-2018-14497	TENDA D152 SSID Cross Site Scripting	A vulnerability, which was classified as problematic, has been found in Tenda D152 (the affected version is unknown). Affected by this issue is an unknown function of the component SSID Handler. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by Default Rules.
		CVE-2018-14937	My Little Forum 2.4.12 Add Page menu link Cross Site Scripting	A vulnerability, which was classified as problematic, has been found in My Little Forum 2.4.12. Affected by this issue is an unknown function of the component Add Page. The manipulation of the argument Menu Link with	Protected by Default Rules.

				an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	
		CVE-2018-14936	My little forum 2.4.12 add page title Cross Site Scripting	A vulnerability classified as problematic was found in My Little Forum 2.4.12. Affected by this vulnerability is an unknown function of the component Add Page. The manipulation of the argument Title with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 45129	PageResponse FB Inboxer Add-on 1.2 - 'search_field' SQL Injection	The vulnerability allows an attacker to inject SQL commands from the search section with 'search_field' parameter in the management panel	Protected by Default Rules.
		CVE-2018-12482	OCS Inventory 2.4.1 Search Engine SQL Injection	A vulnerability classified as critical was found in OCS Inventory 2.4.1. This vulnerability affects an unknown function of the component Search Engine. The manipulation with an unknown input leads to a SQL injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.
3.	Local File Inclusion	EDB-ID: 148759	HRSale 1.0.6 Local File Disclosure	HRSale HR Management PHP script version 1.0.6 suffers from a local file disclosure vulnerability.	Protected by Default Rules.

		EDB-ID: 45128	TI Online Examination System v2 - Arbitrary File Download	The "Export" operation in the admin panel is vulnerable. The attacker can download and read all files known by the name via "download.php"	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2018-14029	WityCMS 0.6.2 - Cross-Site Request Forgery (Password Change)	An authenticated POST request will be generated from victim browser and it will be submitted to the victim.com to modify user's data to attacker desired value.	Protected by Custom Rules.
5.	Command Injection	CVE-2018-14417	SoftNAS Cloud up to 4.0.2 web administration console recent version Command Injection	A vulnerability classified as critical has been found in SoftNAS Cloud up to 4.0.2. Affected is an unknown function of the component Web Administration Console. The manipulation of the argument's recent version as part of a parameter leads to a privilege escalation vulnerability (Command Injection). CWE is classifying the issue as CWE-88. This is going to have an impact on confidentiality, integrity, and availability.	Protected by Default Rules.