Weekly Zero-Day Vulnerability Coverage Bulletin

(6th August – 12th August)

Summary:

Total **15 Zero-Day Vulnerabilities** were discovered in **3 Categories** previous week

12
Cross Site Scripting

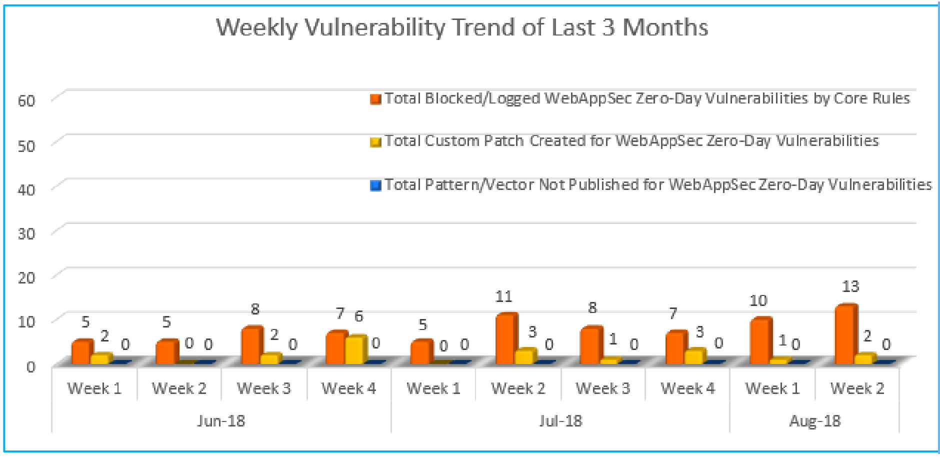
1
Local File Inclusion

2
Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	13
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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

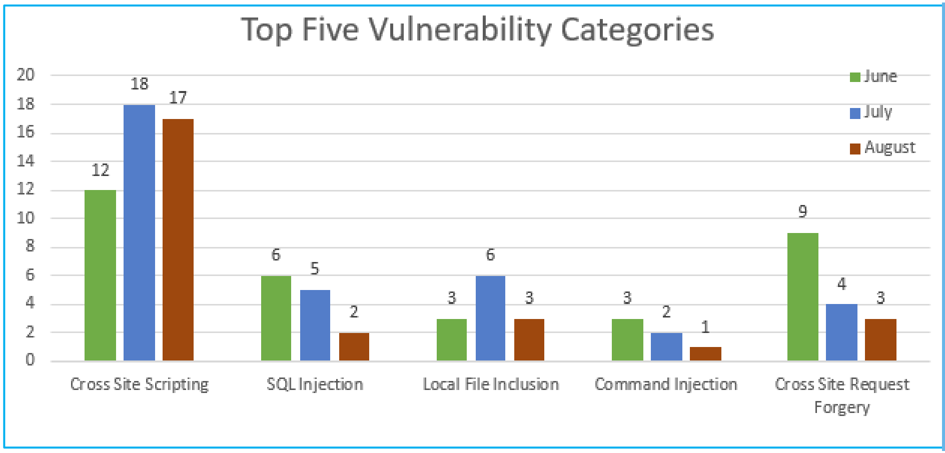
Vulnerability Trend:



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

78% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

22% 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-2018-14493	Open-AudIT Community 2.2.6 - Cross-Site Scripting	Cross-site scripting (XSS) vulnerability on Groups Page in Open-AudIT Community edition in 2.2.6 allows remote attackers to inject arbitrary web script	Protected by Default Rules.
		CVE-2018-14922	Monstra-Dev 3.0.4 Stored Cross Site Scripting	Monstra-Dev 3.0.4 Stored Cross Site Scripting	Protected by Default Rules.
		CVE-2018-14840	Subrion CMS- 4.2.1 XSS (Using component with known Vulnerability)	Subrion CMS- 4.2.1 XSS (Using component with known Vulnerability)	Protected by Default Rules.
		CVE-2018-1690	IBM Rhapsody Model Manager 6.0.6 Web UI cross site scripting	A vulnerability was found in IBM Rhapsody Model Manager 6.0.6. It has been rated as problematic. Affected by this issue is an unknown function of the component *Web UI*. 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	Protected by Default Rules.
		CVE-2018-14976	QCMS 3.0.1 category.php cross site scripting	A vulnerability was found in QCMS 3.0.1. It has been rated as problematic. This issue affects an unknown function of the file *upload/System/Controller/backend/category.php*. 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	Protected by Default Rules.
		CVE-2018-14975	QCMS 3.0.1 album.php cross site scripting	A vulnerability was found in QCMS 3.0.1. It has been declared as problematic. This vulnerability affects	Protected by Default Rules.

		an unknown function of the file *upload/System/Controller/backend/album.php*. The manipulation 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	
CVE-2018-14974	QCMS 3.0.1 news.php cross site scripting	A vulnerability was found in QCMS 3.0.1. It has been classified as problematic. This affects an unknown function of the file *upload/System/Controller/backend/news.php*. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on 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	Protected by Default Rules.
CVE-2018-14973	QCMS 3.0.1 product.php cross site scripting	A vulnerability was found in QCMS 3.0.1 and classified as problematic. Affected by this issue is an unknown function of the file *upload/System/Controller/backend/product.php*. 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	Protected by Default Rules.
CVE-2018-14972	QCMS 3.0.1 down.php cross site scripting	A vulnerability has been found in QCMS 3.0.1 and classified as problematic. Affected by this vulnerability is an	Protected by Default Rules.

		unknown function of the file *upload/System/Controller/backend/down.php*. The manipulation 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	
CVE-2018-14971	QCMS 3.0.1 user.php cross site scripting	A vulnerability, which was classified as problematic, was found in QCMS 3.0.1. Affected is an unknown function of the file *upload/System/Controller/backend/user.php*. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on 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	Protected by Default Rules.
CVE-2018-14970	QCMS 3.0.1 slideshow.php cross site scripting	A vulnerability, which was classified as problematic, has been found in QCMS 3.0.1. This issue affects an unknown function of the file *upload/System/Controller/backend/slideshow.php*. 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	Protected by Default Rules.
CVE-2018-14969	QCMS 3.0.1 system.php cross site scripting	A vulnerability classified as problematic was found in QCMS 3.0.1. This vulnerability affects an unknown function of the	Protected by Default Rules.

				file *upload/System/Controller/backend/system.php*. The manipulation 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	
2.	Local File Inclusion	EDB-ID: 45155	CMS ISWEB 3.5.3 - Directory Traversal	CMS ISWEB 3.5.3 is vulnerable to directory traversal and local file download.	Protected by Default Rules.
3.	Cross Site Request Forgery	EDB-ID: 45154	onArcade Cross-Site Request Forgery (Add Admin)	The application is vulnerable to CSRF attack (No CSRF token in place) meaning that if an admin user can be tricked to visit a crafted URL.	Protected by Custom Rules.
		CVE-2018-14978	QCMS Backend add.html cross site request forgery	A vulnerability classified as problematic was found in QCMS (the affected version is unknown). Affected by this vulnerability is an unknown function of the file *backend/user/admin/add.html* of the component *Backend*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application.	Protected by Custom Rules.