Weekly Zero-Day Vulnerability Coverage Bulletin

(15th October – 21st October)

Summary:

Total **13 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

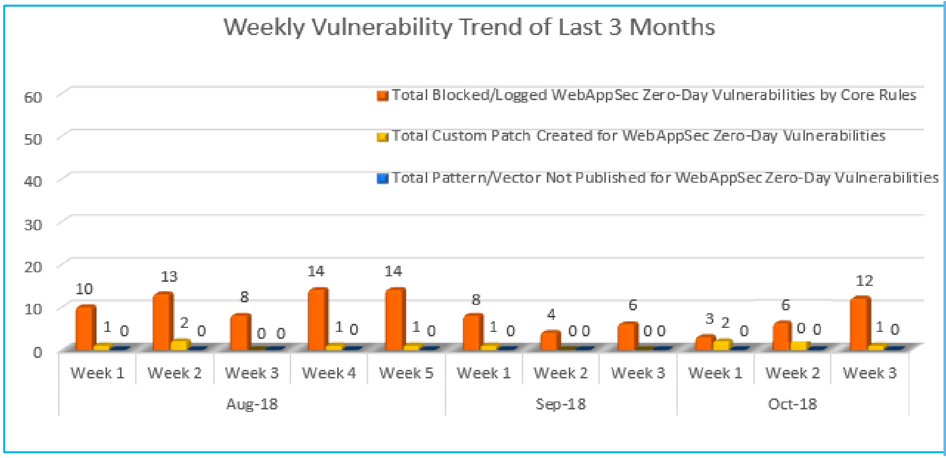
9	1	1	2
Cross Site Scripting	SQL Injection	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	12
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

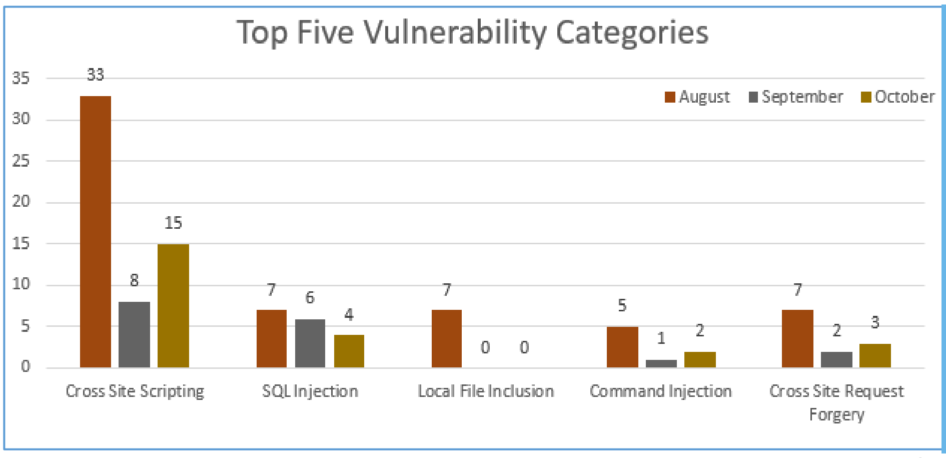
Vulnerability Trend:



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

89% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

11% 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 August compared to other months and categories.

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-2018-18308	BigTree CMS 4.2.23 - Cross-Site Scripting	In the 4.2.23 version of BigTree, a Stored XSS vulnerability has been discovered in /admin/ajax/file-browser/upload/ (aka the image upload area)	Protected by Default Rules.
		CVE-2018-18419	ARDAWAN.COM User Management 1.1 JPG File Name Stored cross site scripting	A vulnerability was found in ARDAWAN.COM User Management 1.1. It has been declared as problematic. This vulnerability affects an unknown function of the component *JPG File Name Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). 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.	Protected by Default Rules.
		CVE-2018-18417	Ekushey Project Manager CRM 3.1 create name cross site scripting	A vulnerability was found in Ekushey Project Manager CRM 3.1. It has been classified as problematic. This affects an unknown function of the file *index.php/admin/client/create*. The manipulation of the argument name as part of a *Parameter* leads to a cross site scripting vulnerability (Stored). 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.	Protected by Default Rules.
		CVE-2018-18416	LANGO Codeigniter Multilingual Script 1.0 Upload admin/settings/update site_name cross site scripting	A vulnerability was found in LANGO Codeigniter Multilingual Script 1.0 and classified as problematic. Affected by this issue is an unknown function of the file *admin/settings/update* of the component	Protected by Default Rules.

		Upload Handler. The manipulation of the argument site_name as part of a *Parameter* 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.	
CVE-2018-15315	F5 BIG-IP up to 12.1.3.6/13.1.1.1 Configuration Utility Page Reflected cross site scripting	A vulnerability classified as problematic was found in F5 BIG-IP up to 12.1.3.6/13.1.1.1. Affected by this vulnerability is an unknown function of the component *Configuration Utility Page*. The manipulation with 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.	Protected by Default Rules.
CVE-2018-15314	F5 BIG-IP AFM up to 12.1.3.6/13.1.1.1 TMUI Reflected cross site scripting	A vulnerability classified as problematic has been found in F5 BIG-IP AFM up to 12.1.3.6/13.1.1.1. Affected is an unknown function of the component *TMUI*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Reflected). 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.	Protected by Default Rules.
CVE- 2018-15313	F5 BIG-IP AFM up to 12.1.3.6/13.1.1.1 TMUI Reflected cross site scripting	A vulnerability was found in F5 BIG-IP AFM up to 12.1.3.6/13.1.1.1. It has been rated as problematic. This issue affects an unknown function of the component *TMUI*. The manipulation with an unknown input leads to	Protected by Default Rules.

				a cross site scripting vulnerability (Reflected). 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	
		CVE-2018-15312	F5 BIG-IP up to 12.1.3.6/13.1.1.1 Configuration Utility Reflected cross site scripting	A vulnerability was found in F5 BIG-IP up to 12.1.3.6/13.1.1.1. It has been declared as problematic. This vulnerability affects an unknown function of the component *Configuration Utility*. The manipulation with 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	Protected by Default Rules.
		CVE-2018-12672	SV3C L-SERIES HD CAMERA V2.3.4.2103-S50-NTD-B20170508B cross site scripting	A vulnerability, which was classified as problematic, was found in SV3C L-SERIES HD CAMERA V2.3.4.2103-S50-NTD-B20170508B. Affected is an unknown function. 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 against	Protected by Default Rules.
2.	SQL Injection	CVE-2018-18527	OwnTicket 2018-05-23 showTicketId/editTicketStatusId sql injection	A vulnerability has been found in OwnTicket 2018-05-23 and classified as critical. This vulnerability affects an unknown function. The manipulation of the	Protected by Default Rules.

				argument showTicketId/editTicketStatusId as part of a *Parameter* 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. The weakness was shared 10/19/2018 as *EDB-ID 45637*	
3.	Cross Site Request Forgery	CVE-2018-18420	Zenario Content Management System 8.3 organizer.ajax.php cross site request forgery	A vulnerability was found in Zenario Content Management System 8.3. It has been rated as problematic. This issue affects an unknown function of the file *admin/organizer.ajax.php?path=zenario__content%2Fpanels%2Fcontent*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was shared in 10/19/2018.	Protected by Custom Rules.
4.	Command Injection	CVE-2018-18382	Advanced HRM up to 1.6 Picture PHP Code Execution privilege escalation	A vulnerability has been found in Advanced HRM up to 1.6 and classified as critical. Affected by this vulnerability is an unknown function of the component *Picture Handler*. The manipulation with an unknown input leads to a privilege escalation vulnerability (PHP Code Execution). The CWE	Protected by Default Rules.

			definition for the vulnerability is CWE-94. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was disclosed 10/16/2018 as *EDB-ID 45604* as uncorroborated exploit (Exploit-DB). It is possible to read	
	CVE-2018-18396	Moxa ThingsPro 2.1 Remote Code Execution [CVE-2018-18396]	A vulnerability, which was classified as critical, was found in Moxa ThingsPro 2.1. Affected is an unknown function. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was shared 10/19/2018. This vulnerability is traded as CVE-2018-18396 since 10/16/2018. It is possible to launch the attack remotely. The technical details are unknown.	Protected by Default Rules.