Weekly Zero-Day Vulnerability Coverage Bulletin

(22nd October – 28th October)

Summary:

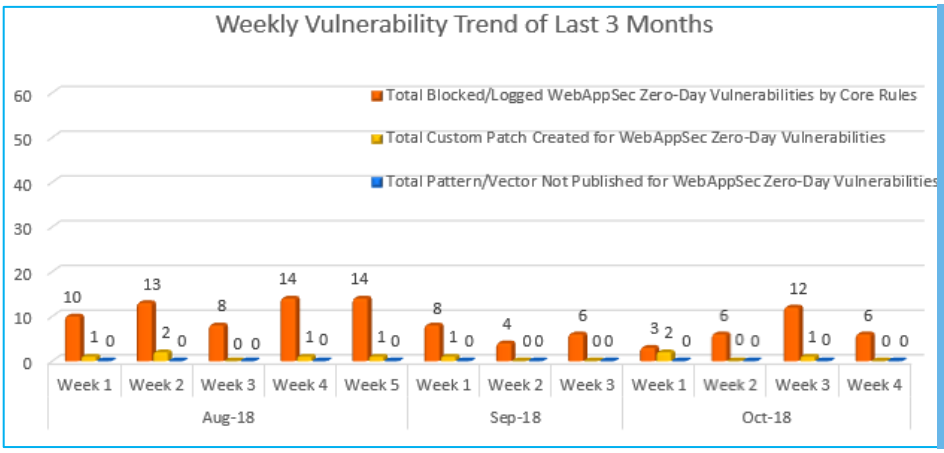
Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** in this week

4	1	1
Cross Site Scripting	SQL Injection	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	6
Zero-Day Vulnerabilities Protected through Custom Rules	0*
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

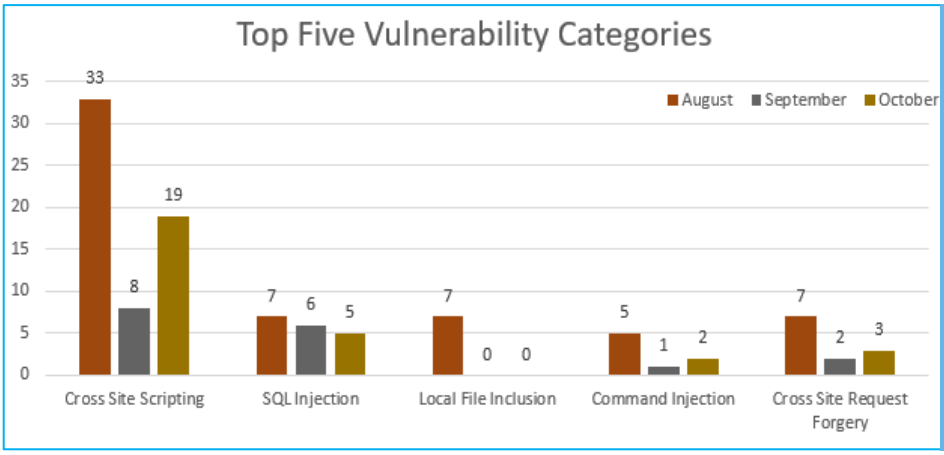
Vulnerability Trend:



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 so far.

Very less SQL Injection attacks were 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-2018-18579	DeDeCMS 5.7 /member/pm.php folder cross site scripting	A vulnerability was found in DeDeCMS 5.7. It has been rated as problematic. Affected by this issue is an unknown function of the file */member/pm.php*. The manipulation of the argument folder as part of a *Parameter* leads to 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.	Protected by Default Rules.
		CVE-2018-18622	Waimai Super CMS 20150505 index.php username cross site scripting	A vulnerability classified as problematic has been found in Waimai Super CMS 20150505. Affected is an unknown function of the file *index.php?m=public&a=doregister*. The manipulation of the argument username as part of a *Parameter* 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.	Protected by Default Rules.
		CVE-2018-18660	Arcserve Unified Data Protection up to 6.5 Update 4 domain.jsp cross site scripting	A vulnerability classified as problematic is found in Cisco Webex Meetings Desktop App on Windows (the affected version is unknown). Affected is an unknown function of the component *Update Service*. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was presented	Protected by Default Rules.

				10/24/2018 as *cisco-sa-20181024-webex-inject* as confirmed advisory (Website). The advisory is shared for download at	
		VE-2018-18660	Arcserve Unified Data Protection up to 6.5 Update 4 domain.jsp cross site scripting	A vulnerability classified as problematic has been found in Cisco Webex Meetings Desktop App on Windows (the affected version is unknown). Affected is an unknown function of the component *Update Service*. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was presented 10/24/2018 as *cisco-sa-20181024-webex-inject* as confirmed advisory (Website). The advisory is shared for download at	Protected by Default Rules.
2.	SQL Injection	CVE-2018-18550	ServersCheck Monitoring Software up to 14.3.3 sql injection [CVE-2018-18550]	A vulnerability was found in ServersCheck Monitoring Software up to 14.3.3 and classified as critical. Affected by this issue is an unknown function. The manipulation with an unknown input lead to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impact is on 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 10/21/2018. This vulnerability is handled as CVE-2018-18550 since 10/21/2018.	Protected by Default Rules.
3.	Command Injection	CVE-2018-18586	libmspack up to 0.7 chmextract Sample Program	A vulnerability was found in libmspack up to 0.7 and classified as critical. Affected by this	Protected by Default Rules.

	chmextract.c CHM File directory traversal [Disputed]	issue is an unknown function of the file *chmextract.c* of the component *chmextract Sample Program*. The manipulation as part of a *CHM File* leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. The impact is on confidentiality, integrity, and availability. The weakness was disclosed 10/23/2018. This vulnerability is handled as CVE-2018-18586 since 10/22/2018.