Weekly Zero-Day Vulnerability Coverage Bulletin

(29th April – 5th May)

Summary:

Total **13 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

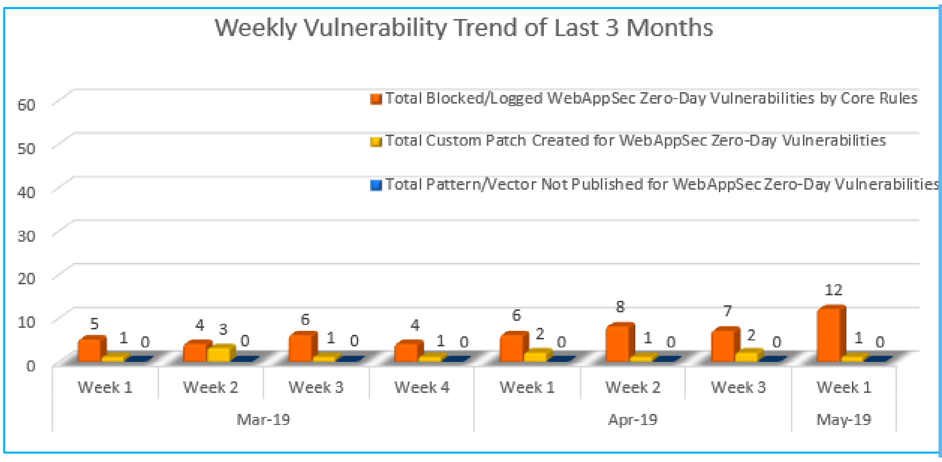
2	**6**	**1**	**3**	**1**
Cross Site Scripting	SQL Injection	Directory Traversal	Command Injection	Cross Site Request Forgery

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

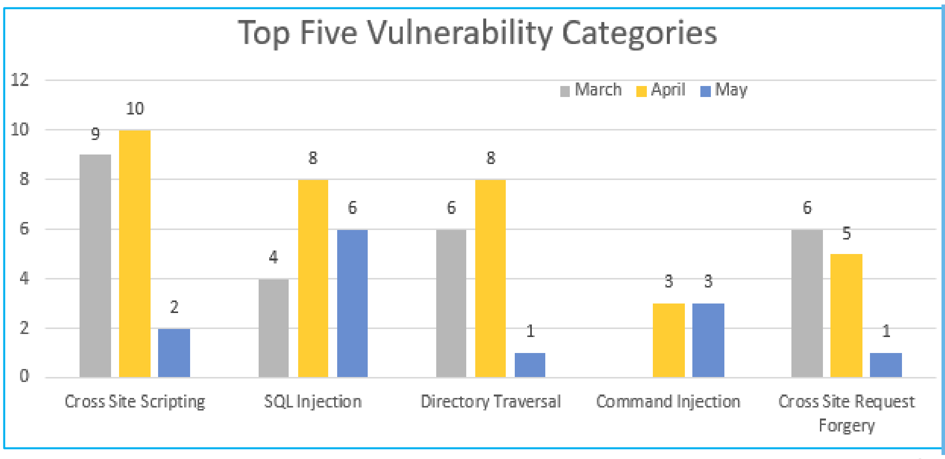
Vulnerability Trend:



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

82% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

18% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting, SQL Injection & Directory Traversal vulnerabilities were discovered in April compared to other months and categories so far.

Zero Command Injection vulnerabilities are found in March.

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-2019-3562	Oculus Browser up to 5.7.11 UI cross site scripting	A vulnerability has been found in Oculus Browser up to 5.7.11 and classified as problematic. Affected by this vulnerability is a functionality of the component *UI*. 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 website. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-11592	WebID 1.2.2 admin/deletenews.php Parameter cross site scripting	A vulnerability, which was classified as problematic, was found in WebID 1.2.2. This affects a function of the file *admin/deletenews.php*. The manipulation as part of a *Parameter* leads to a cross site scripting vulnerability (Reflected). CWE is classifying the issue as CWE-79. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance and would make it possible to initiate further.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-11625	doorGets 7.0 emailingRequest.php sql injection	A vulnerability was found in doorGets 7.0. It has been classified as critical. Affected is code of the file */doorgets/app/requests/user/emailingRequest.php*. The manipulation with an unknown input lead to a sql injection vulnerability. CWE is	Protected by Default Rules.

		classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange. The weakness was presented on 04/30/2019. This vulnerability is traded as CVE-2019-11625 ever since.	
CVE-2019-11623	doorGets 7.0 configurationRequest.php sql injection	A vulnerability has been found in doorGets 7.0 and classified as critical. This vulnerability affects a functionality of the file */doorgets/app/requests/user/configurationRequest.php*. The manipulation with an unknown input lead 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 released in 04/30/2019. This vulnerability was named as CVE-2019-11623.	Protected by Default Rules.
CVE-2019-11622	doorGets 7.0 modulecategoryRequest.php modulecategory_edit_titre sql injection	A vulnerability, which was classified as critical, was found in doorGets 7.0. This affects a function of the file */doorgets/app/requests/user/modulecategoryRequest.php*. The manipulation of the argument modulecategory_edit_titre with an unknown input lead to a sql injection vulnerability. CWE is classifying the issue as	Protected by Default Rules.

		CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange. The weakness was published in 04/30/2019.	
CVE-2019-11621	doorGets 7.0 configurationRequest.php sql injection	A vulnerability, which was classified as critical, has been found in doorGets 7.0. Affected by this issue is some functionality of the file */doorgets/app/requests/user/configurationRequest.php*. The manipulation with an unknown input lead to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange. The weakness was shared in 04/30/2019. This vulnerability is handled as CVE-2019-11621 ever since.	Protected by Default Rules.
CVE-2019-11620	doorGets 7.0 modulecategoryRequest.php modulecategory_add_titre sql injection	A vulnerability classified as critical was found in doorGets 7.0. Affected by this vulnerability is the functionality of the file */doorgets/app/requests/user/modulecategoryRequest.php*. The manipulation of the argument modulecategory_add_titre with an unknown input lead to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to	Protected by Default Rules.

				affect confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange. The weakness was presented in 04/30/2019.	
		CVE-2019-11619	doorGets 7.0 configurationRequest.php sql injection	A vulnerability classified as critical has been found in doorGets 7.0. Affected is an unknown function of the file */doorgets/app/requests/user/configurationRequest.php*. The manipulation with an unknown input lead to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact 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 disclosed in 04/30/2019. This vulnerability is traded as CVE-2019-11619 ever since.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-11624	doorGets 7.0 configurationRequest.php directory traversal	A vulnerability was found in doorGets 7.0 and classified as critical. This issue affects a part of the file */doorgets/app/requests/user/configurationRequest.php*. The manipulation with an unknown input leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. The weakness was disclosed in 04/30/2019. The identification of this vulnerability is CVE-2019-11624 since 04/30/2019.	Protected by Default Rules.

				The attack may be initiated remotely. Technical details of the vulnerability are known, but there is no available exploit.	
4.	Cross Site Request Forgery	CVE-2019-10315	GitHub Authentication Plugin up to 0.31 on Jenkins Oauth state cross site request forgery	A vulnerability, which was classified as problematic, was found in GitHub Authentication Plugin up to 0.31 on Jenkins (Bug Tracking Software). Affected is a function of the component *Oauth*. The manipulation of the argument state as part of a *Parameter* leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application.	Protected by Custom Rules.
5.	Command Injection	CVE-2019-3493	Micro Focus Network Automation up to 2018.11 Remote Code Execution	A vulnerability classified as critical was found in Micro Focus Network Automation up to 2018.11. This vulnerability affects the functionality. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published in 04/29/2019. The advisory is shared for download at softwaresupport.softwaregrp.com. This vulnerability was named CVE-2019-3493 since 12/31/2018. The attack can be initiated remotely.	Protected by Default Rules.

CVE-2019-3926	Crestron AM-100/AM-101 SNMP System Command command injection	A vulnerability, which was classified as very critical, was found in Crestron AM-100 and AM-101. Affected is a function of the component *SNMP*. The manipulation as part of a *System Command* 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. CVE summarizes:Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to command injection via SNMP OID iso.3.6.1.4.1.3212.100.3.2.14.1.	Protected by Default Rules.
CVE-2019-3925	Crestron AM-100/AM-101 SNMP System Command command injection	A vulnerability, which was classified as very critical, has been found in Crestron AM-100 and AM-101. This issue affects some functionality of the component *SNMP*. The manipulation as part of a *System Command* leads to a privilege escalation vulnerability (Command Injection). Using CWE to declare the problem leads to CWE-88. Impacted is confidentiality, integrity, and availability. The summary by CVE is:Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to command injection via SNMP OID iso.3.6.1.4.1.3212.100.3.2.9.3.	Protected by Default Rules.