Product Newsletter

May 2019 Edition

Web Application Scanning

On the WAS side, our effort was to build upon the new scanner that we recently released and add plugins that improve coverage. Some of the major advances made on WAS side are as follows:

Signature Updates

Signatures were added to find the following new vulnerabilities

1

Cookie Scoped To Parent Domain:
A cookie scoped to the parent domain will be available to all subdomains therefore increasing the chance of leakage. This may occur when the information is transmitted unencrypted or when a XSS vulnerability affected a subdomain is in place.

2

Oracle WebLogic Server Deserialization Remote Command Execution Vulnerability (CVE-2019-2725
Oracle WebLogic servers includes wls9_async_response.war and wls-wsat.war packages by default which provides asynchronous communication for WebLogic Server service. These WAR packages can be misused when deserializing input information and an attacker can send a constructed malicious HTTP request to gain the permissions of the target server and execute the command remotely without authorization.

3

Apache Tomcat Remote Code Execution Vulnerability (CVE-2019-0232)
A vulnerability in the CGI Servlet of Apache Tomcat could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system. The vulnerability occurs when enableCmdLineArguments is enabled on a Windows system and the Java Runtime Environment (JRE) passes command-line arguments to the system. An attacker could exploit this vulnerability by passing command-line arguments to the affected system. A successful exploit could allow the attacker to execute code on the targeted system.

4

Credit Card Number Disclosed:
Sensitive financial information such as Credit Card Number has been found in HTTP response. Credit Card Number disclosure may allow remote attackers to steal other financial information and make unknown transactions.

5

WordPress XML-RPC Interface Detected
XML-RPC is a remote procedure call (RPC) protocol which uses XML to encode its calls and HTTP as a transport mechanism. "XML-RPC" also refers generically to the use of XML for a remote procedure call, independently of the specific protocol. A public facing WordPress XML-RPC interface has been detected. An attacker may exploit this issue to execute arbitrary commands or code in the context of the web server. This may facilitate various attacks, including unauthorized remote access.

Portal Updates

1

Scope Edited in Application Audit Reports:
The scope of the automated reports were edited to provide more information. Now if website is configured for authenticated scan then in the scope customer would see the following statement under scope in AA reports

"Indusface has conducted Application Scan on web applications using valid credentials".

2

Severity & CVSS Score update along with CVSS vector
All vulnerabilities were updated with CVSS v3 Score along with the CVSS vector. This is done to make the severities and CVSS score match industry standard and make it comparable. Now the severity of the vulnerabilities would match the CVSS score provided. It would be based on the following guidance

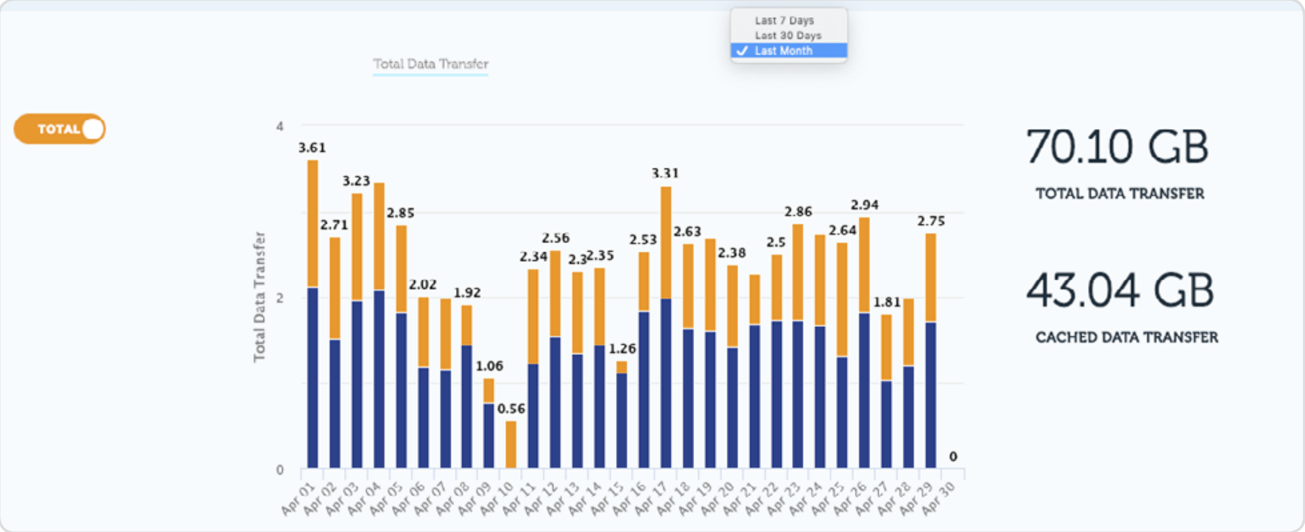
0 - Info
0.1 - 3.9 Low
4.0 - 6.9 - Medium
7.0 - 8.9 - High
9.0 - 10.0 – Critical

Please be adviced, due to this change customers might see some change in severity of some vulnerabilities.

AppTrana

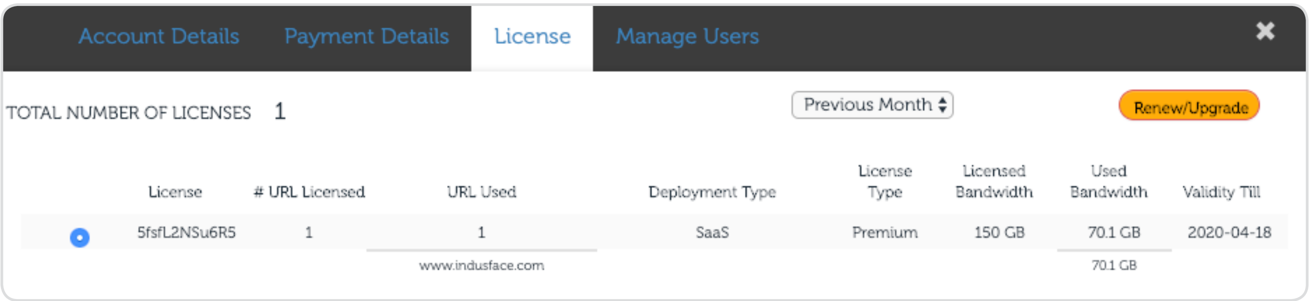
Portal Updates

Now customer can see the bandwidth usage for last month directly from the portal. They can view it website wise.



As you already know we charge only for clean traffic, so customer can readily validate the traffic calculation by checking the access logs in application server and see if monthly data matches with what they see in the portal

Similarly one can get license wise bandwidth information from the license page



TOTAL NUMBER OF LICENSES 1

	License	# URL Licensed	URL Used	Deployment Type	License Type	Licensed Bandwidth	Used Bandwidth	Validity Till
●	5fsfL2NSu6R5	1	1	SaaS	Premium	150 GB	70.1 GB	2020-04-18
			www.indusface.com				70.1 GB	

Bugs Fixed

- Daily Summary Mail will go only for websites assigned to user instead of all websites that are part of customer account.
- Charges for extra GB will happen automatically during next billing cycle for customers who have onboarded using CC
- Logged in Customer Admin can update his Name, Mail id and can enable/Disable 2FA from Manage user page .
- 'Scan behind Login page' functionality has been enabled for Basic website.
- LetsEncrypt modify button has been enabled. Now Customer can update LetEncrypt certificate to Custom SSL certificate from Apptrana Setting page.