[R1] Tenable.sc 5.17.0 Fixes Multiple Vulnerabilities

Medium

← View more security advisories

Synopsis

Tenable.sc leverages third-party software to help provide underlying functionality. Two separate third-party components (jQuery and OpenSSL) were found to contain vulnerabilities, and updated versions have been made available by the providers.

Out of caution and in line with good practice, Tenable opted to upgrade the bundled libraries to address the potential impact of these issues. Tenable.sc version 5.17.0 will update jQuery to 3.5.1 and OpenSSL to 1.1.1i to address the identified vulnerabilities.

Additionally, Tenable.sc 5.17.0 will also address an Access Control issue within the Automatic Distribution configuration. In certain scenarios, a scanner could potentially be used outside the user's defined scan zone for a scan without a particular zone being specified.

Solution

Tenable has released Tenable.sc 5.17.0 to address these issues. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/tenable-sc).

This page contains information regarding security vulnerabilities that may impact Tenable's products. This may include issues specific to our software, or due to the use of third-party

of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2020-11022
CVE-2020-1971
CVE-2020-1967
CVE-2019-1551
CVE-2020-5808
Tenable Advisory ID: TNS-2020-11
Risk Factor: Medium
Credit:
Justin LaSelva (CVE-2020-5808)
CVSSv2 Base / Temporal Score
4.3 / 3.4 (CVE-2020-11022)
4.3 / 3.4 (CVE-2020-1971)
5.0 / 4.1 (CVE-2020-1967)
5.0 / 4.1 (CVE-2019-1551)
4.3 / 3.4 (CVE-2020-5808)
CVSSv2 Vector:
(AV:N/AC:M/Au:N/C:N/I:P/A:N)(CVE-2020-11022)
(AV:N/AC:M/Au:N/C:N/I:N/A:P)(CVE-2020-1971)
(AV:N/AC:L/Au:N/C:N/I:N/A:P)(CVE-2020-1967)
(AV:N/AC:L/Au:N/C:P/I:N/A:N)(CVE-2019-1551)
(AV:N/AC:M/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)(CVE-2020-5808)

Affected Products

Tenable.sc versions < 5.17.0

Advisory Timeline

2020-12-21 - [R1] Initial Release

Featured products

Tenable One Exposure Management Platform

Tenable Cloud Security (CNAPP)

Tenable Cloud Vulnerability Management

Tenable CIEM

Tenable Vulnerability Management

Tenable Security Center

Tenable Web App Scanning

Tenable Patch Management

Tenable Enclave Security

Tenable Attack Surface Management

Tenable Nessus

Tenable AI Exposure

Tenable OT Security

Tenable Identity Exposure

View all ›

Featured solutions

Active Directory

Building management systems

Cloud security posture management

Compliance

Exposure management

Banks and financial services

Healthcare

State / Local / Education

US federal

Vulnerability management

Zero trust

View all ›

Customer resources

Resource library

Exposure management resources

Community & support

Customer education

Tenable Research

Documentation

Cybersecurity guide

Why Tenable

Trust

System status

Connections

Blog

Contact us

Careers

Investors

Tenable Ventures

Events

Media

508 compliance