[R1] Tenable.sc 5.21.0 Fixes Multiple Third-Party Vulnerabilities

Critical

← View more security advisories

Synopsis

Tenable.sc leverages third-party software to help provide underlying functionality. Several of the third-party components were found to contain vulnerabilities, and updated versions have been made available by the providers.

Out of caution, and in line with best practice, Tenable has upgraded the bundled components to address the potential impact of these issues. Tenable.sc 5.21.0 updates the following components to address the identified vulnerabilities:

jQuery UI upgraded from 1.12.0 to 1.13.1
MomentJS upgraded from 2.29.1 to 2.29.2
PHP upgraded from 8.0.12 to 8.0.16
Apache upgraded from 2.4.52 to 2.4.53
OpenSSL upgraded from 1.1.1(L) to 1.1.1(n)

Solution

Tenable has released Tenable.sc 5.21.0 to address these issues. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/tenable-sc).

Additional References

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 libraries within our software. Tenable strongly encourages users to ensure that they upgrade or apply relevant patches in a timely manner.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one 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-2022-0778
CVE-2022-23943
CVE-2022-24828
CVE-2021-41116
CVE-2021-41182
CVE-2021-41183
CVE-2021-41184
CVE-2022-24785
CVE-2021-21707
Tenable Advisory ID: TNS-2022-09
Risk Factor: Critical
CVSSv3 Base / Temporal Score:
7.5 / 6.5 (CVE-2022-0778)
9.8 / 8.5 (CVE-2022-23943)
8.3 / 7.5 (CVE-2022-24828)
9.8 / 8.8 (CVE-2021-41116)
6.1 / 5.3 (CVE-2021-41182)
6.1 / 5.3 (CVE-2021-41183)
6.1 / 5.3 (CVE-2021-41184)
7.5 / 6.5 (CVE-2022-24785)
5.3 / 4.6 (CVE-2021-21707)

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C (CVE-2021-41116)
AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:U/RL:O/RC:C (CVE-2021-41182)
AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:U/RL:O/RC:C (CVE-2021-41183)
AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:U/RL:O/RC:C (CVE-2021-41184)
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C (CVE-2022-24785)
AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C (CVE-2021-21707)

Affected Products

Tenable.sc versions 5.20.0 and earlier

Advisory Timeline

2022-04-20 - [R1] Initial Release

>

Featured solutions

Active Directory

Building management systems

Cloud security posture management

Compliance

Exposure management

Banks and financial services

Healthcare

Hybrid cloud security

IT/OT

Ransomware

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