[R1] Stand-alone Security Patch Available for Tenable.sc versions 5.19.0 to 5.20.1: Patch 202204.1

Critical

← View more security advisories

Synopsis

Tenable.sc leverages third-party software to help provide underlying functionality. Two of the third-party components (Apache and OpenSSL) 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 Patch 202204.1 updates OpenSSL to version 1.1.1n and Apache to version 2.4.53 to address the identified vulnerabilities.

Solution

Tenable has released Tenable.sc Patch 202204.1 to address these issues. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/tenable-sc).

Additional References

https://docs.tenable.com/releasenotes/Content/tenablesc/tenablesc2022041.htm
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778

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
Tenable Advisory ID: TNS-2022-08
Risk Factor: Critical
CVSSv3 Base / Temporal Score:
7.5 / 6.5 (CVE-2022-0778)
9.8 / 8.5 (CVE-2022-23943)
CVSSv3 Vector:
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C (CVE-2022-0778)
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C (CVE-2022-23943)

Affected Products

Tenable.sc 5.19.0, 5.19.1, 5.20.0, and 5.20.1

Advisory Timeline

2022-04-06 - [R1] Initial Release

>

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

Hybrid cloud security

IT/OT

Ransomware

State / Local / Education

US federal

Vulnerability management