



Try



[R1] Nessus Network Monitor 6.0.0 Fixes Multiple Third-party Vulnerabilities

Critical

← View more security advisories

Synopsis

Nessus Network Monitor leverages third-party software to help provide underlying functionality. One of the third-party components (OpenSSL) was found to contain vulnerabilities, and updated versions have been made available by the providers.

Out of caution and in line with best practice, Tenable opted to upgrade the bundled OpenSSL components to address the potential impact of these issues. Nessus Network Monitor 6.0.0 updates OpenSSL to version 1.1.1l to address the identified vulnerabilities.

Solution

Tenable has released Nessus Network Monitor 6.0.0 to address these issues. The installation files can be obtained from the Tenable Downloads Portal (<https://www.tenable.com/downloads/nessus-network-monitor>).

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



Try



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

Risk Information

CVE ID: [CVE-2021-3711](#)

[CVE-2021-3712](#)

Tenable Advisory ID: TNS-2022-02

Risk Factor: Critical

CVSSv3 Base / Temporal Score:

9.8 / 8.5 (CVE-2021-3711)

7.4 / 6.4 (CVE-2021-3712)

CVSSv3 Vector:

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C (CVE-2021-3711)

AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C (CVE-2021-3712)

Affected Products

Nessus Network Monitor versions 5.13.1 and earlier

Advisory Timeline

2022-01-05 - [R1] Initial Release

>



Featured products

Tenable One Exposure Management Platform

Tenable Cloud Security (CNAPP)

Tenable Cloud Vulnerability Management

Tenable CIEM

Tenable Vulnerability Management

[Try](#)

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
Zero trust

View all >

Customer resources

Resource library



Try



- Tenable Research
- Documentation
- Cybersecurity guide
- Why Tenable
- Trust
- System status

Connections

- Blog
- Contact us
- Careers
- Investors
- Tenable Ventures
- Events
- Media

-
- Privacy policy
 - Do not sell/share my personal information
 - Legal
 - 508 compliance

© 2026 Tenable®, Inc. All rights reserved

