[R1] Nessus Network Monitor 5.13.0 Fixes One Third-party Vulnerability

Medium

← View more security advisories

Synopsis

Nessus Network Monitor leverages third-party software to help provide underlying functionality. One of the third-party components (jQuery) was 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 jQuery components to address the potential impact of these issues. Nessus Network Monitor 5.13.0 updates jQuery to version 3.5.1 to address the identified vulnerabilities.

Solution

Tenable has included a fix in Nessus Network Monitor 5.13.0 to address this issue. 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

guidelines page.

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

Risk Information

CVE ID: CVE-2020-11022
CVE-2020-11023
Tenable Advisory ID: TNS-2021-02
Risk Factor: Medium
CVSSv2 Base / Temporal Score
4.3 / 3.4
CVSSv2 Vector:
(AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Affected Products

NNM 5.12.1 and earlier

Advisory Timeline

2021-02-17 - [R1] Initial Release

>

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

Exposure management resources

Community & support

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