



Try



[R1] Nessus 8.13.0 Fixes One Third-party Vulnerability

Medium

[← View more security advisories](#)

Synopsis

Nessus 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 8.13.0 updates jQuery to version 3.5.1 to address the identified vulnerabilities.

Solution

Tenable has included a fix in Nessus 8.13.0 to address this issue. The installation files can be obtained from the Tenable Downloads Portal (<https://www.tenable.com/downloads/nessus>).

Additional References

<https://docs.tenable.com/releasenotes/Content/nessus/nessus8130.htm>

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.



Try



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](#)

Tenable Advisory ID: TNS-2020-10

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

Nessus 8.12.1

Advisory Timeline

2020-12-07 - [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

[Try](#)

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

Exposure management resources



Try



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

