[R1] Nessus Agent Version 11.1.3 Fixes Arbitrary File Deletion

High

← View more security advisories

Synopsis

A vulnerability has been identified in Nessus Agent on Windows where an attacker to create a junction, enabling the deletion of arbitrary files with SYSTEM privileges. As a result, this condition potentially facilitates arbitrary code execution, whereby an attacker may exploit the vulnerability to execute malicious code with elevated SYSTEM privileges.

Solution

Tenable has released Nessus Agent 11.1.3 to address this issues. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/nessus-agents).

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.

Risk Information

CVE ID: CVE-2026-33694
Tenable Advisory ID: TNS-2026-12
Risk Factor: High
CVSSv3 Base / Temporal Score:
8.2 / 7.4
CVSSv3 Vector:
AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSSv4 Base Score:
7.4
CVSSv4 Vector:
CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P
CWE:
CWE-59: Improper Link Resolution Before File Access ("Link Following")

Affected Products

Nessus Agent 11.1.2 and earlier

Disclosure Timeline

2025-12-29 - Report received by Tenable.
2026-2-18 - Report was accepted by Tenable.
2026-03-23 - CVE ID requested / CVSS Scoring calculated
2026-4-23 - Nessus Agent 11.1.3 released.

Advisory Timeline

2026-4-23 - [R1] Initial Release

>

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
Zero trust

Resource library
Exposure management resources
Community & support
Customer education
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