مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Nessus

Tracking #:432318849

Date:28-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity vulnerability has been identified in Tenable's Nessus & Nessus Agent for Windows systems.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in Tenable's Nessus & Nessus Agent for Windows systems. Tracked as CVE-2026-33694, this flaw allows a locally authenticated attacker to exploit improper link resolution using Windows junctions. Successful exploitation can result in arbitrary file deletion with SYSTEM-level privileges, potentially leading to privilege escalation and arbitrary code execution.

Vulnerability Details:

- CVE ID: CVE-2026-33694
- 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")

Patched Versions:

- Nessus 10.11.4
- Nessus 10.12.0
- Nessus Agent 11.1.3

RECOMMENDATIONS:

- Upgrade Immediately: Upgrade Nessus & Nessus Agent to fixed version at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://tenable.com/security/tns-2026-13
- https://tenable.com/security/tns-2026-12