مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Tenable Nessus Agent (Windows)

Tracking #:432318222

Date:09-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Tenable has disclosed a high-severity local privilege escalation vulnerability affecting the Nessus Agent Tray Application on Windows hosts.

TECHNICAL DETAILS:

Tenable has disclosed a high-severity local privilege escalation vulnerability affecting the Nessus Agent Tray Application on Windows hosts. The issue arises from improper handling during the installation and uninstallation process, allowing a locally authenticated attacker with low privileges to escalate to higher system privileges.

Vulnerability Details:

- CVE ID: CVE-2025-36640
- CVSS v3 Base Score: 8.8
- Tenable Advisory ID: TNS-2026-01
- Severity: High
- Risk Factor: High
- Affected Platform: Windows
- Affected Component: Nessus Agent Tray Application (installation/uninstallation routines)
- Attack Type: Local Privilege Escalation

Affected Products

- Nessus Agent versions prior to 10.9.3
- Nessus Agent versions 11.0.0 through 11.0.2

Fixed Versions

- Nessus Agent 10.9.3
- Nessus Agent 11.0.3

RECOMMENDATIONS:

- Upgrade Nessus Agent immediately to one of the mentioned patched versions.

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://www.tenable.com/security/tns-2026-01