مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Nessus Manager

Tracking #:432318505

Date:03-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Tenable has released security updates addressing a high-severity path traversal vulnerability in Nessus Manager.

TECHNICAL DETAILS:

Tenable has released security updates addressing a high-severity path traversal vulnerability in Nessus Manager. The vulnerability, tracked as CVE-2026-3493, allows an authenticated remote attacker to read arbitrary operating system files on affected installations.

Vulnerability Details

- **CVE ID:** CVE-2026-3493
- **Advisory ID:** TNS-2026-08
- **Severity:** High
- **CWE Classification:** CWE-35 – Path Traversal

Affected Products

- Nessus Manager 10.10.2 and earlier
- Nessus Manager 10.11.0 through 10.11.2

Fixed Versions

- Nessus Manager 10.10.3
- Nessus Manager 10.11.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Nessus Manager to the latest or fixed version.

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-2026-08