مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates for Nessus Windows Hosts

Tracking #:432317464

Date:08-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Tenable has released security updates for Nessus windows hosts versions to remediate critical vulnerabilities affecting both internal functionality and third-party components (libxml2 and libxslt).

TECHNICAL DETAILS:

Tenable has released Nessus versions 10.8.5 and 10.9.0 to remediate critical vulnerabilities affecting both internal functionality and third-party components (libxml2 and libxslt). These vulnerabilities include a high-severity local privilege escalation (CVE-2025-36630), and potential denial of service or code execution risks due to outdated XML libraries. Immediate action is recommended to avoid system compromise, particularly on Windows hosts.

Vulnerability Details:

1. CVE-2025-36630 — Local Privilege Escalation in Nessus (Windows)
   - Description: Non-admin users can overwrite arbitrary local system files with Nessus logs using SYSTEM-level privileges
   - Impact: Local privilege escalation and system compromise
   - CVSS v3.1: 8.4 (Base) / 7.6 (Temporal)
   - Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H
   - Risk Factor: High

2. CVE-2025-6021 — libxml2 XML Parsing Vulnerability
   - Component: libxml2
   - Description: Malformed XML inputs could cause a denial of service
   - Fixed Version: libxml2 v2.13.8 (backported into Nessus 10.8.5)
   - CVSS v3.1: 6.5 (Base) / 5.7 (Temporal)
   - Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   - Risk Factor: Medium

3. CVE-2025-24855 — libxslt Code Execution Risk
   - Component: libxslt
   - Description: Improper handling of XSL transformations could lead to privilege escalation
   - Fixed Version: libxslt v1.1.43
   - CVSS v3.1: 7.8 (Base) / 6.8 (Temporal)
   - Vector: AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H
   - Risk Factor: High

Affected Products:

- Nessus 10.8.4 and earlier

Fixed Versions:

- Nessus 10.8.5
- Nessus 10.9.0

RECOMMENDATIONS:

The UAE Cyber Security council recommends to upgrade Nessus to fixed versions 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://www.tenable.com/security/tns-2025-13