مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Buffer Overflow Vulnerability in Net-SNMP

Tracking #:432318171

Date:24-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability has been identified in Net-SNMP, a widely deployed open-source network monitoring and management suite.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in Net-SNMP, a widely deployed open-source network monitoring and management suite. The flaw, tracked as CVE-2025-68615, affects the snmptrapd daemon, a core component responsible for receiving SNMP trap messages.

Vulnerability Details:

- **CVE ID:** CVE-2025-68615
- **Severity:** Critical CVSS score of 9.8
- **Vulnerability Type:** Buffer Overflow
- **Affected Component:** snmptrapd daemon
- **Affected Software:** Net-SNMP (all versions prior to patch)
- The vulnerability is triggered when the snmptrapd service processes a malformed SNMP trap packet. Due to improper bounds checking, this input causes a buffer overflow, leading to a crash of the daemon.

Fixed Version:

- 5.9.5, 5.10.pre2.

RECOMMENDATIONS:

- Upgrade Immediately- Upgrade Net-SNMP to one of the mentioned fixed 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://github.com/net-snmp/net-snmp/security/advisories/GHSA-4389-rwqf-q9gq