مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Critical Vulnerability in GNU telnetd

Tracking #:432318318

Date:28-01-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical authentication bypass vulnerability was disclosed in the GNU Inetutils telnetd daemon that is actively exploited in the wild, allowing remote attackers to gain unauthorized access without valid credentials.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability, tracked as CVE-2026-24061, was publicly disclosed in January 2026 affecting the telnetd daemon in GNU Inetutils (versions from 1.9.3 through 2.7). This flaw allows unauthenticated remote attackers to bypass login authentication and gain root-level access by injecting the "-f root" flag via the USER environment variable during Telnet session negotiation. Assigned a CVSS v3.1 score of 9.8 (Critical), the vulnerability enables direct remote code execution as root with no credentials required.

Vulnerability Details

- CVE ID: CVE-2026-24061
- CVSS v3.1: 9.8 (CRITICAL)
- CWE: CWE-88 – Improper Neutralization of Argument Delimiters in a Command (Argument Injection)

Affected Vendor and Product

- Vendor: GNU
- Product: InetUtils – telnetd
- Affected Versions: 1.9.3 through 2.7
- Default Status: Affected

Root Cause

- The vulnerability arises from improper sanitization of user-controlled environment variables during the Telnet authentication process.
- Specifically, telnetd improperly processes the USER environment variable, allowing attackers to inject arguments.

RECOMMENDATIONS:

- Apply vendor patches or updated packages as soon as they become available.
- If no patch is available, remove GNU InetUtils telnetd entirely.
- Replace Telnet with SSH or other encrypted remote-access protocols.

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.cve.org/CVERecord?id=CVE-2026-24061