مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Unpatched RCE Vulnerability in GNU InetUtils Telnetd

Tracking #:432318632

Date:20-03-2026

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in GNU InetUtils telnetd that allows an unauthenticated remote attacker to execute arbitrary code on affected systems during the Telnet session negotiation phase.

TECHNICAL DETAILS:

A critical security vulnerability (CVE-2026-32746) has been identified in GNU InetUtils telnetd. The flaw allows an unauthenticated remote attacker to execute arbitrary code on affected systems by sending a specially crafted message during the TELNET session negotiation phase.
Due to the lack of authentication requirements and the high impact of successful exploitation, this vulnerability poses a significant risk, particularly to legacy environments where TELNET is still in use.

Vulnerability Details

- **CVE ID:** CVE-2026-32746
- **Severity:** Critical **CVSS v3.1 Score:** 9.8)
- The vulnerability is caused by improper bounds checking in the handling of the LINEMODE SLC (Set Local Characters) option within the TELNET protocol. An attacker can exploit this flaw by sending a maliciously crafted SLC suboption during the initial connection handshake, before authentication occurs.
- This results in a buffer overflow condition that can be leveraged to achieve remote code execution with root privileges. The attack requires no user interaction or credentials and can be triggered with a single network connection to the TELNET service (TCP port 23).

Affected Products

- GNU InetUtils telnetd
- **Affected Versions:** All versions up to and including 2.7

Systems potentially impacted include:

- Linux distributions (e.g., Debian, Ubuntu, RHEL, SUSE) with telnetd enabled
- Embedded systems and IoT devices exposing TELNET services
- Industrial Control Systems (ICS) and Operational Technology (OT) environments
- Servers or network appliances listening on TCP port 23

Fixed Versions

- Currently No official patch available
- A security patch is expected to be released by April 1, 2026

Mitigations (Until Patch is Available)

- Disable the Telnet service if it is not required
- Avoid running telnetd with root privileges
- Block or restrict TCP port 23 at network and host levels
- Limit Telnet access to trusted IP addresses or internal networks only
- Isolate systems running Telnet services from critical infrastructure

RECOMMENDATIONS:

- Identify and inventory systems running telnetd

- Immediately apply mitigations to reduce exposure
- Monitor network traffic for suspicious Telnet activity
- Apply vendor patches as soon as they become available
- Replace Telnet with secure alternatives such as SSH where possible
- Conduct security assessments to detect potential compromise

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://nvd.nist.gov/vuln/detail/CVE-2026-32746
- https://dreamgroup.com/vulnerability-advisory-pre-auth-remote-code-execution-via-buffer-overflow-in-telnetd-linemode-slc-handler/#