



An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2603190012

NCSC Advisory

Critical Vulnerability exists in GNU Inetutils
telnetd

CVE-2026-32746

19th, March 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>.
Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-32746**Published:** 2026-03-13**Vendor:** GNU**Product:** inetutils**CVSS Score¹:** 9.8

Products Affected

Product	Version
inetutils	0 <= 2.7

Impact

telnetd in GNU inetutils through 2.7 allows an out-of-bounds write in the LINEMODE SLC (Set Local Characters) suboption handler because add_slc does not check whether the buffer is full.

Any unauthenticated attacker with network access to port 23 can trigger the overflow with a single telnet connection and a crafted SLC suboption.

Successful exploitation can lead to arbitrary code execution as root and full compromise of the host.

Common Weakness Enumeration (CWE)²: CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

¹ <https://www.first.org/cvss/>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from GNU.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-32746>
- <https://www.cve.org/CVERecord?id=CVE-2026-32746>
- <https://lists.gnu.org/archive/html/bug-inetutils/2026-03/msg00031.html>

