CVE-2026-32746

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-32746
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-13 19:55:10 UTC
Updated	2026-05-05 18:15:51 UTC
Description	telnetd in GNU inetutils through 2.7 allows an out-of-bounds write in the LINEMODE SLC (Set Local Characters) suboption

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from cve@mitre.org

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000330000 probability, percentile 0.093490000 (date 2026-05-05)

Problem Types: CWE-120 | CWE-120 CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Inetutils	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GNU	Inetutils	affected 2.7 custom	Not specified

References

Reference	Source	Link	Tags
github.com/watchtowrlabs/watchtowr-vs-telnetd-CVE-2026-32746	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Third I
lists.gnu.org/archive/html/bug-inetutils/2026-03/msg00031.html	cve@mitre.org	lists.gnu.org	Exploi
www.openwall.com/lists/oss-security/2026/03/12/4	cve@mitre.org	www.openwall.com	Mailin
www.openwall.com/lists/oss-security/2026/03/14/1	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailin
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**