

CVE-2026-24061

GNU InetUtils Argument Injection Vulnerability

Exigent

CISA KEV since Jan 26, 2026

Actively exploited

Public exploit module (Metasploit)

telnetd in GNU Inetutils through 2.7 allows remote authentication bypass via a "-f root" value for the USER environment variable.

EVRS 89/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.990 99.93rd percentile · FIRST	CISA DEADLINE Feb 16, 2026 CISA federal deadline · Overdue by 8 months
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.990 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
inetutils	≥ 1.9.3 ≤ 2.7	no fixed version listed	NVD
debian linux	11.0	no fixed version listed	NVD

Sources

Vendor guidance	codeberg.org/inetutils/inetutils/commit/ccba9f748aa8d50a38d7748e2e60362edd6a32cc	Additional guidance	lists.gnu.org/archive/html/bug-inetutils/2026-01/msg00004.html
cggit.git.savannah.gnu.org	cggit.git.savannah.gnu.org/cggit/inetutils.git	codeberg.org	codeberg.org/inetutils/inetutils/commit/fd702c02497b2f398e739e3119bed0b23dd7aa7b
NVD	nvd.nist.gov/vuln/detail/CVE-2026-24061	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-3688	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-24061

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.