AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Vulnerabilitet kritik i pa patchuar i RCE në GNU InetUtils Telnetd

Data 25/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Një dobësi kritike në GNU InetUtils telnetd që lejon një sulmues të paautorizuar në distancë të ekzekutojë kod arbitrar në sistemet e prekura.

Informacione Teknike

Një dobësi kritike sigurie (CVE-2026-32746) është identifikuar në GNU InetUtils telnetd. Kjo dobësi i lejon një sulmuesi të paautorizuar në distancë të ekzekutojë kod arbitrar në sistemet e prekura duke dërguar një mesazh të hartuar posaçërisht gjatë fazës së negociatave të sesionit TELNET.
Për shkak të mungesës së kërkesave të autentifikimit dhe ndikimit të lartë të shfrytëzimit të suksesshëm, kjo dobësi paraqet një rrezik të konsiderueshëm, veçanërisht për mjediset ku TELNET është ende në përdorim.

Detajet e dobësisë
• ID e CVE: CVE-2026-32746
• Ashpërsia: Kritike (Pikët CVSS v3.1: 9.8)
• Dobësia shkaktohet nga kufijtë e papërshtatshëm që kontrollojnë trajtimin e opsionit LINEMODE SLC (Vendos Karakteret Lokale) brenda protokollit TELNET. Një sulmues mund ta shfrytëzojë këtë dobësi duke dërguar një nënopsion SLC të hartuar me qëllim keqdashës gjatë lidhjes fillestare, përpara se të ndodhë autentifikimi.
• Kjo rezulton në një gjendje mbingarkese buffer që mund të shfrytëzohet për të arritur ekzekutimin e kodit në distancë me privilegje root. Sulmi nuk kërkon ndërveprim ose kredenciale nga përdoruesi dhe mund të shkaktohet me një lidhje të vetme rrjeti me shërbimin TELNET (porta TCP 23).

Produktet e Prekura
• GNU InetUtils telnetd
• Versionet e Prekura: Të gjitha versionet deri në dhe duke përfshirë 2.7
Sistemet që potencialisht preken përfshijnë:
• Shpërndarjet Linux (p.sh., Debian, Ubuntu, RHEL, SUSE) me telnetd të aktivizuar
• Sistemet e integruara dhe pajisjet IoT që ekspozojnë shërbimet TELNET
• Sistemet e Kontrollit Industrial (ICS) dhe mjediset e Teknologjisë Operacionale (OT)
• Serverat ose pajisjet e rrjetit që dëgjojnë në portin TCP 2a
Versionet e përditësuar
• Aktualisht Nuk ka asnjë patch zyrtar të disponueshëm
• Një patch sigurie pritet të publikohet deri më 1 Prill 2026

Mitigimet (Derisa Patch të jetë i Disponueshëm)
• Çaktivizoni shërbimin Telnet nëse nuk kërkohet
• Shmangni ekzekutimin e telnetd me privilegje root

• Bllokoni ose kufizoni portin TCP 23 në nivelet e rrjetit dhe hostit
• Kufizoni aksesin e Telnet vetëm në adresat IP të besuara ose rrjetet e brendshme
• Izoloni sistemet që ekzekutojnë shërbime Telnet nga infrastruktura kritike

Rekomandime

AKSK rekomandon

Identifikoni dhe inventarizoni sistemet që përdorin telnetd

• Zbatoni menjëherë mitigimet për të zvogëluar ekspozimin
• Monitoroni trafikun e rrjetit për aktivitet të dyshimtë Telnet
• Zbatoni patch-et e shitësve sapo ato të bëhen të disponueshme
• Zëvendësoni Telnet me alternativa të sigurta si SSH aty ku është e mundur
• Kryeni vlerësime sigurie për të zbuluar kompromentime të mundshme