THREAT BULLETINS

Active Exploitations of an 11-Year-Old Critical Telnetd Vulnerability (CVE-2026-24061)

TLP:WHITE

Jan 27, 2026

On January 19, 2026, a security researcher, Kyu Neushwaistein (a.k.a. Carlos Cortes Alvarez), reported an 11-year-old critical vulnerability in **telnetd**, tracked as **CVE-2026-24061**.

The vulnerability, with a CVSS score of 9.8, is an authentication bypass flaw that allows root access via Telnet. It has been discovered to be actively weaponized by actors like **'rwxrwx'**.

Therefore, healthcare providers must disable Telnet (especially if not in use), update to v2.7-2+, or isolate unpatchable equipment via strict network segmentation to prevent any malicious payloads and data theft.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability.

Analysis

CVE-2026-24061 is a critical authentication-bypass vulnerability (CVSS 9.8) in the **GNU InetUtils telnetd** service that resurfaced in

2026 as a major threat to healthcare infrastructure. This 'ghost bug' stems from the unsanitized handling of the **'USER'** environment variable, allowing an attacker to inject the **'-f root'** argument to bypass password prompts entirely. For the health sector, this is particularly perilous because Telnet remains a frequent, albeit legacy, presence in **Operational Technology (OT)** and **Internet of Medical Things (IoMT)** devices, such as older patient monitors, infusion pumps, and legacy lab equipment that lack modern security protocols, such as SSH.

The vulnerability is being weaponized by threat actors, including **'rwxrwx'** who shared a link to an exploit from an open source, posted by a security researcher, Kyu Neushwaistein (Carlos Cortes Alvarez), that automates root-level access. In the healthcare environment, the risk is amplified by the sector's reliance on **long-lifecycle equipment** that often remains in service for 15+ years. Active campaigns are currently using this bypass to deploy secondary payloads, such as **reverse shells** and **persistent backdoors**. Because many medical devices run on monolithic or unpatchable firmware, a single exposed Telnet port can serve as an entry point for lateral movement into sensitive Electronic Health Record (EHR) networks, potentially leading to data exfiltration or ransomware.

Healthcare organizations must treat this as an immediate patient safety risk and prioritize **disabling Telnet (Port 23)** across all clinical and administrative networks. If a legacy medical device requires Telnet for functionality, it should be isolated within a strictly segmented VLAN with no external internet access and restricted internal routing. Furthermore, IT teams should, where possible, update **GNU InetUtils to version 2.7-2** or higher and deploy **Endpoint Detection and Response (EDR)** tools to monitor for unauthorized shell spawning by telnetd processes. Continuous monitoring for 'pre-authenticated' root sessions in system logs is essential for identifying active breaches that bypass traditional credential-based alerts.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- **Decommission Telnet (if applicable):** Telnet is a legacy, clear-text protocol. Immediately disable telnetd services (Port 23 and 2323) across all clinical and administrative networks, if applicable.
- **Prioritize Patching:** Update GNU InetUtils to version 2.7-2 or higher. If you are using a specific Linux distribution (Debian, Ubuntu, etc.), verify their latest backports for the 'sanitize-expansions' patch.
- **Sanitize Login Environment:** If Telnet cannot be removed, configure the daemon to use a custom login wrapper that explicitly blocks or strips the -f (force) argument from the USER variable.
- **IoMT Segmentation (VLANs):** Place older medical devices (infusion pumps, patient monitors) on strictly isolated VLANs. Use a Default-Deny policy at the network level to block all outbound traffic and restrict inbound access to specific authorized management consoles.
- **Device Lifecycle Inventory:** Use a proper device/asset inventory system, such as Software Bill of Materials (SBOM), to identify legacy devices running GNU InetUtils. Given the 15-year lifecycle of medical equipment, many 'black box' devices may be vulnerable without appearing so.
- **Threat Monitoring and Hunting:** Monitor for instances of '/usr/bin/login' being executed with the '-f' flag by the telnetd process.
- **Network Detection:** Deploy NIDS signatures for 'NEW-ENVIRON' Telnet options containing the string 'USER=-f root'.
- **Endpoint Defense:** Ensure that Endpoint Detection and Response (EDR) tools are active on any medical gateways or jump hosts to detect unauthorized shell spawning or secondary payloads, such as reverse shells.
- **Reviewing the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

Reference(s)	greynoise, openwall, hhs, securityaffairs

Sources
https://www.openwall.com/lists/oss-security/2026/01/20/2

https://securityaffairs.com/187255/security/11-year-old-critical-telnetd-flaw-found-in-gnu-inetutils-cve-2026-24061.html

https://viz.greynoise.io/tags/gnu-inetutils-telnetd-authentication-bypass-cve-2026-24061-attempt

Alert ID a2da8412

View Alert

Share Feedback
was this helpful? |

Tags CVE-2026-24061, telnetd service, exploit, Telnet, Authentication Bypass

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**