Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Instant Root Access via CVE-2026-24061: A Decade-Old Bug Comes Alive

Date of Publication	Admiralty Code	TA Number
January 28, 2026	A1	TA2026025

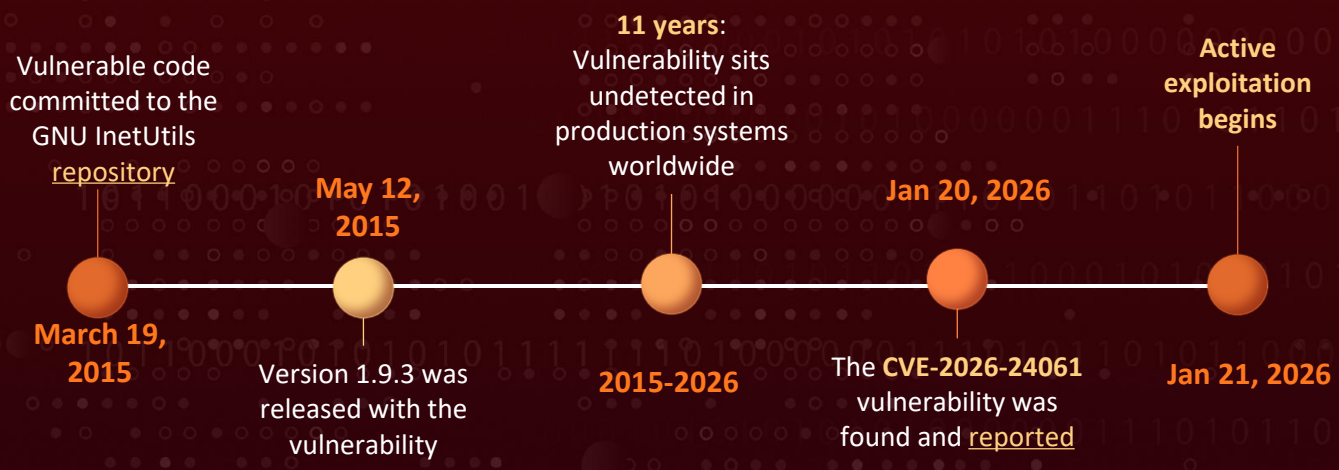
Summary

First Seen: January 19, 2026
Affected Products: GNU InetUtils telnetd
Impact: The successful exploitation of CVE-2026-24061 poses an extremely high risk to organizations running vulnerable GNU InetUtils telnetd services. Attackers gaining root-level access without authentication can execute arbitrary commands, install persistent backdoors through SSH key injection, deploy malware, and exfiltrate sensitive data, and pivot laterally within networks to compromise additional systems. The trivial nature of exploitation, combined with the availability of public proof-of-concept code, significantly lowers the barrier for attackers of all skill levels. Organizations with exposed Telnet services face immediate risk of complete system compromise, and given the legacy nature of Telnet deployments, affected systems may include critical infrastructure components, embedded systems, network appliances, and OT-adjacent environments where rapid patching may be challenging.

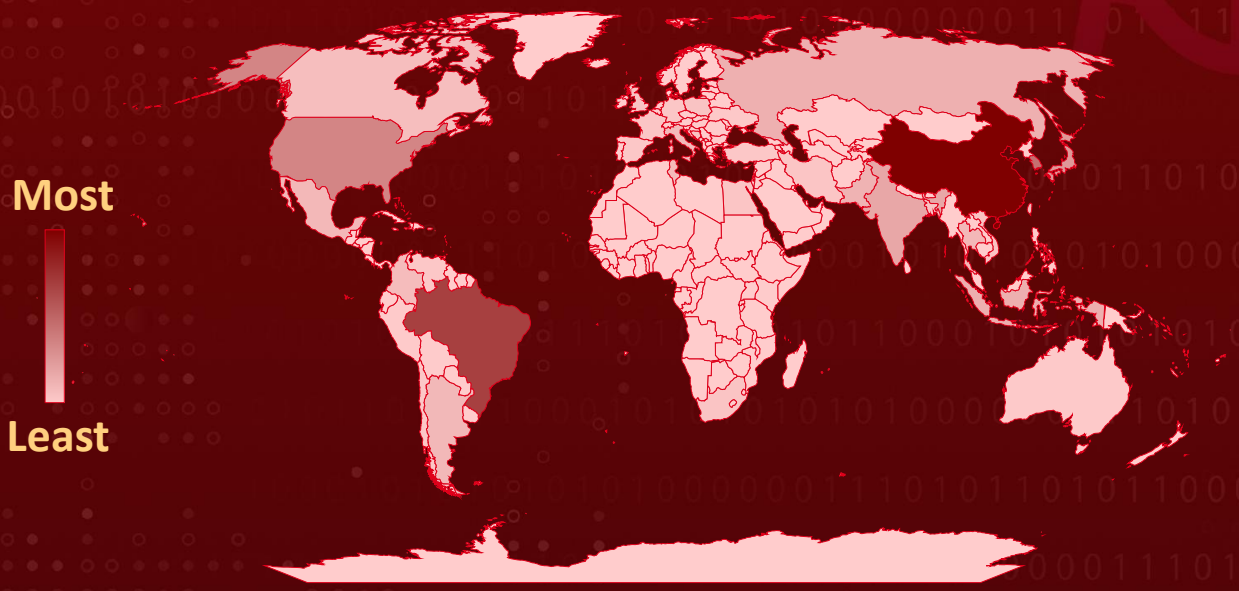
CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-24061	GNU InetUtils Argument Injection Vulnerability	GNU InetUtils telnetd	✗	✓	✓

Exploitation Timeline



Targeted Regions



Vulnerability Details

#1

A severe remote authentication bypass has been uncovered in the telnetd component of GNU InetUtils, tracked as CVE-2026-24061. The flaw allows any unauthenticated remote attacker to gain instant root access by exploiting a long-standing argument injection bug in how the Telnet daemon handles the 'USER' environment variable.

#2

The issue originates from a commit introduced in March 2015. A code change added '%U' expansion to the command template used to invoke '/usr/bin/login'. During Telnet session negotiation, clients are permitted to supply environment variables. Telnetd retrieves the 'USER' value via 'getenv("USER")' and inserts it directly into the login command line without validation or sanitization.

#3

This oversight enables a clean and devastating exploit. By setting the 'USER' variable to '-f root', an attacker injects the '-f' (force login) flag into the login invocation. The login binary interprets this flag as an instruction to skip authentication entirely and immediately grant a shell for the specified user. The result is a root shell with no password, no credentials, and no interaction.

#4 All GNU InetUtils versions from 1.9.3 through 2.7 are affected. The vulnerability has a remote attack vector, requires no privileges, no user interaction, and carries total impact across confidentiality, integrity, and availability. Beyond authentication bypass, attackers can also set arbitrary environment variables for child processes spawned by telnetd, enabling further compromise through mechanisms such as 'PATH' manipulation.

#5 Exploitation was observed within 18 hours of public disclosure. Telemetry captured 60 exploitation attempts across 18 unique attacker IP addresses, spanning Hong Kong, the United States, Japan, the Netherlands, China, Germany, Singapore, and Thailand. Approximately 800,000 Telnet servers remain exposed globally, creating a broad and immediate attack surface.

#6 Post-compromise behavior confirms automated abuse. Attackers executed system reconnaissance commands, injected SSH public keys to establish persistence, and attempted to retrieve second-stage Python malware from external infrastructure. Over 83% of observed attacks explicitly targeted root access. The exploit itself fits on a single line and requires no specialized tooling.

#7 This is a textbook argument injection vulnerability. User-supplied input is passed directly to a privileged binary with zero checks. No filtering. No escaping. No safeguards. The bug remained dormant for nearly 11 years in widely deployed code. Telnet is still common in OT/ICS environments, embedded systems, legacy routers, and unmaintained infrastructure, where patching is rare or nonexistent. The lesson is not subtle: a trivial input-handling flaw silently granted universal root access for over a decade.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-24061	GNU InetUtils telnetd versions 1.9.3 - 2.7	cpe:2.3:a:gnu:inetutils:*:*:*:*:*:*:*:*	CWE-88

Recommendations

Apply Vendor Patches Immediately: GNU InetUtils telnetd should upgrade to version 2.8 or later without delay. The GNU InetUtils maintainers have released patches that sanitize all variables before expansion, addressing both the authentication bypass and the broader environment variable injection issues. For systems unable to upgrade to 2.8, apply the specific security commits (fd702c02497b2f398e739e3119bed0b23dd7aa7b and ccba9f748aa8d50a38d7748e2e60362edd6a32cc) from the Codeberg repository.

Disable Telnet Services Where Possible: Telnet is a legacy protocol that transmits data, including credentials in cleartext, and should not be used in modern environments. Organizations should disable telnetd services entirely and migrate to secure alternatives such as SSH for remote administration. This recommendation aligns with long-standing security best practices and eliminates the vulnerability.

Implement Network-Level Access Controls: If immediate patching or service discontinuation is not feasible, restrict network access to Telnet services at the perimeter firewall level. Block incoming connections to TCP port 23 from untrusted networks and configure firewall rules to allow Telnet access only from explicitly trusted IP addresses or network segments. This reduces the attack surface while permanent remediation is implemented.

Monitor for Indicators of Compromise: Security teams should review logs for signs of exploitation attempts targeting Telnet services, particularly connection attempts with unusual USER environment variable values containing "-f" flags.

Audit SSH Authorized Keys: Given observed post-exploitation activities involving SSH key injection, administrators should audit ~/.ssh/authorized_keys files on all potentially affected systems for unauthorized entries. Any unfamiliar SSH public keys should be removed immediately, and affected user passwords should be rotated. Consider implementing file integrity monitoring on authorized_keys files to detect future unauthorized modifications.

Inventory Telnet-Enabled Systems: Conduct a comprehensive asset inventory to identify all systems running Telnet services across the organization, including network devices, embedded systems, and legacy infrastructure. Use the Shadowserver Foundation's Accessible Telnet Report to identify externally exposed instances. Prioritize remediation based on exposure level and system criticality.

Implement Custom Login Workaround: As a temporary workaround for systems that cannot be immediately patched, configure telnetd to use a custom login wrapper that does not support the -f parameter. This prevents the authentication bypass while allowing Telnet services to continue functioning for operational requirements during the remediation window.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Credential Access	T1552: Unsecured Credentials	T1552.004: Private Keys
Execution	T1059: Command and Scripting Interpreter	T1059.006: Python
Persistence	T1098: Account Manipulation	**T1098.004**: SSH Authorized Keys
Discovery	T1082: System Information Discovery	
	T1087: Account Discovery	**T1087.001: Local Account**
	T1033: System Owner/User Discovery	
Command and Control	T1071: Application Layer Protocol	**T1071.001: Web Protocols**

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	178[.]16[.]53[.]82, 216[.]106[.]186[.]24, 149[.]88[.]75[.]211, 156[.]238[.]237[.]103, 167[.]172[.]111[.]135, 165[.]22[.]30[.]48, 66[.]90[.]99[.]202, 67[.]220[.]95[.]16, 203[.]155[.]222[.]145, 103[.]151[.]172[.]31, 45[.]87[.]43[.]148, 213[.]93[.]218[.]8, 40[.]124[.]112[.]175, 183[.]6[.]91[.]54, 223[.]254[.]128[.]15, 104[.]28[.]222[.]46, 38[.]145[.]220[.]204, 45[.]143[.]233[.]138

Patch Links

https://codeberg.org/inetutils/inetutils/commit/fd702c02497b2f398e739e3119bed0b23dd7aa7b

https://codeberg.org/inetutils/inetutils/commit/ccba9f748aa8d50a38d7748e2e60362edd6a32cc

https://cgit.git.savannah.gnu.org/cgit/inetutils.git

References

https://seclists.org/oss-sec/2026/q1/89

https://www.safebreach.com/blog/safebreach-labs-root-cause-analysis-and-poc-exploit-for-cve-2026-24061/

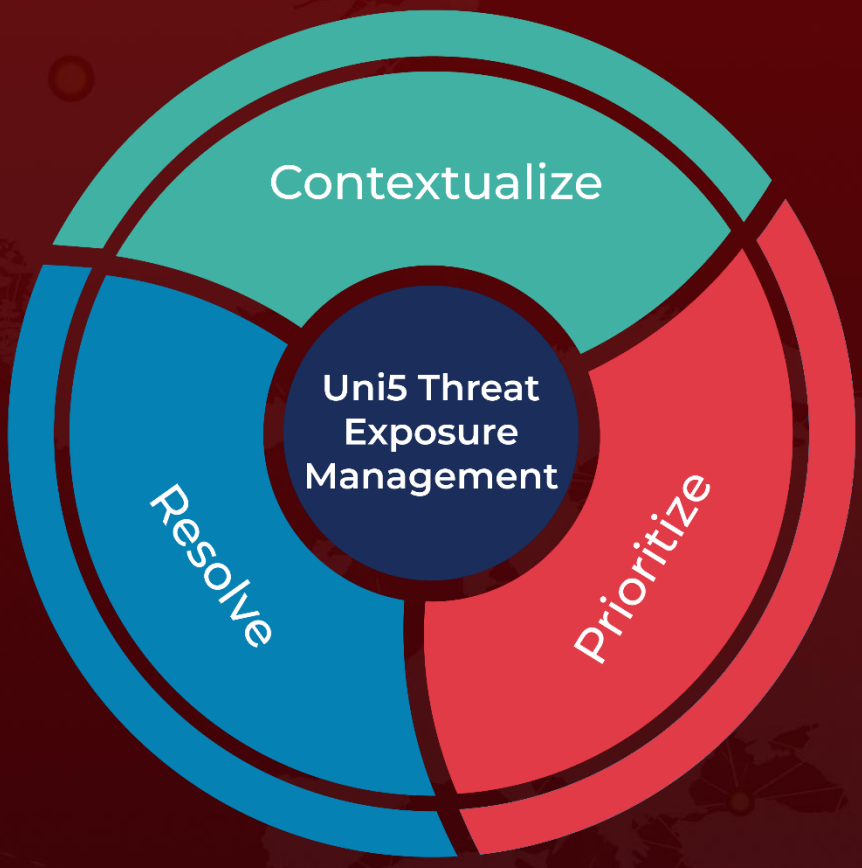
https://www.labs.greynoise.io/grimoire/2026-01-22-f-around-and-find-out-18-hours-of-unsolicited-houseguests/index.html

https://codeberg.org/inetutils/inetutils/commit/fa3245ac8c288b87139a0da8249d0a408c4dfb87

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 28, 2026 • 03:00 AM

More at www.hivepro.com