Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

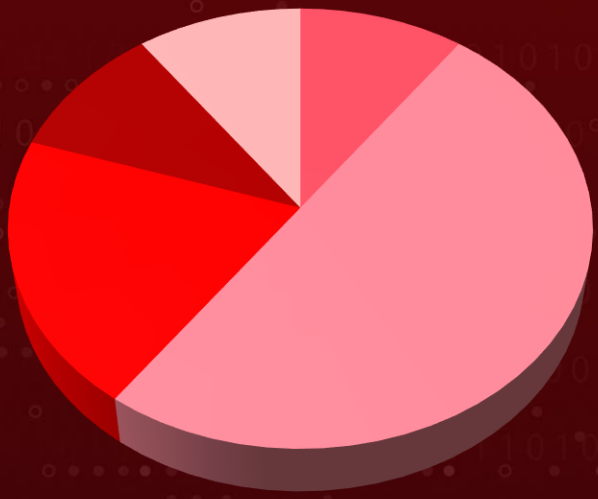
February 2026 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
February 24, 2026	A1	TA2026053

Summary

In February, more than **381** new vulnerabilities were discovered and addressed across the Linux ecosystem, affecting several major distributions, including Debian, Red Hat, OpenSUSE, and Ubuntu. During this period, over **3080** vulnerabilities were also highlighted, with corresponding hotfixes or patches released to resolve them. These vulnerabilities span from information disclosure to privilege escalation to code execution. HiveForce Labs has identified 10 severe vulnerabilities that are exploited or have a high potential of successful exploitation, necessitating immediate attention. To ensure protection, it is essential to upgrade systems to the latest version with the necessary security patches and appropriate security controls.

Threat Distribution



Adversary Tactics

CVEs

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2026-24061*	GNU InetUtils Argument Injection Vulnerability	GNU InetUtils	Authentication Bypass	Remote
CVE-2026-2441*	Google Chromium CSS Use-After-Free Vulnerability	Google Chromium	Code Execution	Remote
CVE-2007-4559	Python Directory Traversal Vulnerability	Python	Overwrite Arbitrary Files	Network
CVE-2023-51385	OpenSSH OS Command Injection Vulnerability	OpenSSH	Command Injection	Network
CVE-2026-27475	SPIP Insecure Deserialization Vulnerability	SPIP	Code Execution	Network
CVE-2025-14009	NLTK Arbitrary Code Execution Vulnerability	NLTK	Code Execution	Network
CVE-2025-65791	ZoneMinder Command Injection Vulnerability	ZoneMinder	Command Injection	Network

* Refers to **Notable CVEs**, vulnerabilities that are either exploited in zero-day attacks, included in the CISA KEV catalog, utilized in malware operations, or targeted by threat actors in their campaigns.

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-69872	DiskCache Unsafe Pickle Deserialization Vulnerability	DiskCache	Code Execution	Local
CVE-2025-15467	OpenSSL Stack Buffer Overflow Vulnerability	OpenSSL	Code Execution	Network
CVE-2025-40778	BIND 9 Cache poisoning attacks with unsolicited RRs Vulnerability	BIND 9	Cache Poisoning	Network

* Refers to **Notable CVEs**, vulnerabilities that are either exploited in zero-day attacks, included in the CISA KEV catalog, utilized in malware operations, or targeted by threat actors in their campaigns.

Notable CVEs

Notable CVEs include vulnerabilities exploited in zero-day attacks, listed in the CISA KEV catalog, used in malware operations, or targeted by threat actors in their campaigns.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-24061	✗ ZERO-DAY	GNU InetUtils telnetd versions 1.9.3 - 2.7	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:gnu:inetutils:*:*:*:*:*:*:*:*	-
GNU InetUtils Argument Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-88	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1098: Account Manipulation, T1082: System Information Discovery	Ubuntu, SUSE, Debian, GNU InetUtils, GNU InetUtils, GNU InetUtils

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-2441	✗	Google Chrome (Before 145.0.7632.75 on Windows/macOS; Before 144.0.7559.75 on Linux)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium CSS Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1189: Drive-By Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	Chrome

Vulnerability Details

#1

In February, the Linux ecosystem underwent an extensive security overhaul, with more than 3080 vulnerabilities addressed across multiple distributions and associated products. Among them, over 381 flaws were newly identified and remediated, spanning high-impact categories such as information disclosure, privilege escalation, and remote code execution. During this review cycle, HiveForce Labs highlighted 10 critical vulnerabilities that are either actively exploited in the wild or assessed as highly likely to be weaponized in the near term.

#2

Collectively, these flaws enable adversarial tactics aligned with Initial Access, Execution, and Privilege Escalation. Notably, two of the identified vulnerabilities are already under active exploitation, significantly elevating organizational risk and underscoring the need for accelerated patch management and exposure reduction.

#3

CVE-2026-24061 affects GNU Inetutils' telnetd service through version 2.7. The flaw allows a remote authentication bypass by supplying a crafted -f root value to the USER environment variable, effectively granting unauthenticated root access.

#4

CVE-2026-2441 is a use-after-free vulnerability in the CSS component of Google Chrome before version 145.0.7632.75. By exploiting a memory corruption condition via a crafted HTML page, a remote attacker can achieve arbitrary code execution within the browser sandbox. The flaw resides in the Chromium rendering engine, and Google has confirmed active exploitation in the wild, making immediate browser updates critical.

#5

CVE-2007-4559, despite being disclosed in 2007, continues to resurface due to Python's ubiquity across Linux distributions. The vulnerability affects the tarfile.extract() and tarfile.extractall() functions, enabling directory traversal through '..' sequences embedded in TAR archive filenames. This can result in arbitrary file overwrite during extraction. With a CVSS v3.1 score of 9.8 (Critical), the flaw remains relevant because Python is deeply integrated into system tooling and application stacks, repeatedly reintroducing risk where secure extraction practices are not enforced.

#6

CVE-2023-51385 is a command injection vulnerability in the client-side component of OpenSSH. The issue manifests when the ProxyCommand directive processes hostnames containing shell metacharacters, such as backticks, without adequate sanitization before passing them to the shell. An attacker can embed arbitrary commands in the hostname, enabling command execution on the client system. Public proof-of-concept exploits were released shortly after disclosure, accelerating the likelihood of exploitation in real-world scenarios.

#7

CVE-2025-14009 impacts the NLTK downloader component in all versions of nltk/nltk. The _unzip_iter function leverages zipfile.extractall() without path validation, allowing attackers to craft malicious ZIP archives that execute arbitrary code when extracted. Several Linux distributions have yet to release patches, leaving dependent systems exposed, particularly in data science and research environments where NLTK is widely used.

#8

CVE-2025-65791 affects ZoneMinder v1.36.34, where unsanitized user input is passed directly to the exec() function in web/views/image.php, resulting in command injection. This vulnerability creates a direct pathway to remote code execution. Some Linux distributions are still pending patches, extending the exposure window.

#9

CVE-2025-69872 concerns DiskCache (python-diskcache) through version 5.6.3, which relies on Python's pickle module for default serialization. If an attacker gains write access to the cache directory, they can introduce malicious serialized objects that trigger arbitrary code execution when deserialized by the application. Patch availability remains inconsistent across distributions.

#10

Several of these vulnerabilities remain unpatched in certain Linux distributions, prolonging organizational exposure. Systems that delay remediation, particularly those running internet-facing services or widely deployed libraries, remain at heightened risk of compromise. Immediate updates, service hardening, and, where feasible, temporary mitigation controls are essential to reduce the attack surface while vendor patches are finalized and deployed.

Recommendations

Proactive Strategies:

- Eliminate High-Risk Legacy Services: Immediately decommission Telnet services; replace with hardened SSH configurations. Block inbound Telnet (TCP/23) at perimeter firewalls and internal segmentation gateways. Enforce secure configuration baselines for GNU Inetutils deployments.
- Aggressive Patch & Version Governance: Implement automated patch orchestration across Linux distributions. Track third-party libraries (Python modules, NLTK, DiskCache, ZoneMinder, OpenSSH clients). Enforce browser version compliance policies to prevent use of vulnerable Chrome builds.
- Restrict Privilege & Execution Surfaces: Apply least privilege across services and applications. Disable root login wherever possible. Restrict write permissions on cache directories and system-critical paths.
- Archive & File Handling Governance: Disallow automatic extraction of untrusted TAR/ZIP archives. Implement content validation and sandboxing for file ingestion workflows. Introduce checksum and signature validation for downloaded packages.
- Harden Development & Application Security Practices: Prohibit unsafe deserialization (e.g., Python pickle in production contexts). Replace extractall() usage with validated extraction logic that enforces path sanitization. Validate and sanitize all user-controlled input before passing to exec() or shell contexts. Enforce secure coding guardrails via SAST/DAST and dependency scanning.

Reactive Strategies:

- Immediate Containment: Isolate affected systems from the network. Disable compromised accounts and rotate credentials. Remove exposed Telnet services immediately.
- Credential & Key Hygiene: Rotate SSH keys across affected infrastructure. Reset passwords for potentially impacted users. Revoke API tokens and service credentials.
- Persistence & Lateral Movement Checks: Look for newly created admin users. Identify scheduled tasks, cron jobs, or system services added post-compromise. Audit SSH configs for malicious ProxyCommand entries. Monitor unusual internal east-west traffic.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-24061	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1098: Account Manipulation, T1082: System Information Discovery	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1026: Privileged Account Management, M1030: Network Segmentation, M1045: Code Signing	✓ Ubuntu, SUSE, Debian
CVE-2026-2441	T1189: Drive-By Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	DET0176: Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy, DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software, M1050: Exploit Protection	✓ Chrome
CVE-2007-4559	T1059: Command and Scripting Interpreter	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1045: Code Signing	✓ Ubuntu, SUSE, Redhat, Amazon ✗ Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2023-51385	T1059: Command and Scripting Interpreter	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1045: Code Signing, M1047: Audit	✓ Ubuntu, SUSE, Debian, Redhat, Amazon
CVE-2026-27475	T1059: Command and Scripting Interpreter	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1045: Code Signing	✓ Debian, ✗ Ubuntu
CVE-2025-14009	T1059: Command and Scripting Interpreter	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1045: Code Signing	✗ Ubuntu, Debian, Redhat
CVE-2025-65791	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse, DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)	M1045: Code Signing, M1038: Execution Prevention, M1016: Vulnerability Scanning	✗ Debian
CVE-2025-40778	T1584: Compromise Infrastructure	DET0885: Detection of Compromise Infrastructure	M1056: Pre-compromise	✓ Ubuntu, SUSE, Debian, Redhat, Amazon

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-69872	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing, T1574: Hijack Execution Flow	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse, DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)	M1045: Code Signing, M1016: Vulnerability Scanning, M1038: Execution Prevention	SUSE, Ubuntu, Debian, Redhat
CVE-2025-15467	T1190: Exploit Public-Facing, T1203: Exploitation for Client Execution	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1035: Limit Access to Resource Over Network, M1016: Vulnerability Scanning	Ubuntu, SUSE, Debian, Redhat, Amazon

References

https://lore.kernel.org/linux-cve-announce/

https://github.com/leonov-av/linux-patch-wednesday

https://www.debian.org/security/#DSAS

https://lists.ubuntu.com/archives/ubuntu-security-announce/

https://access.redhat.com/security/security-updates/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/

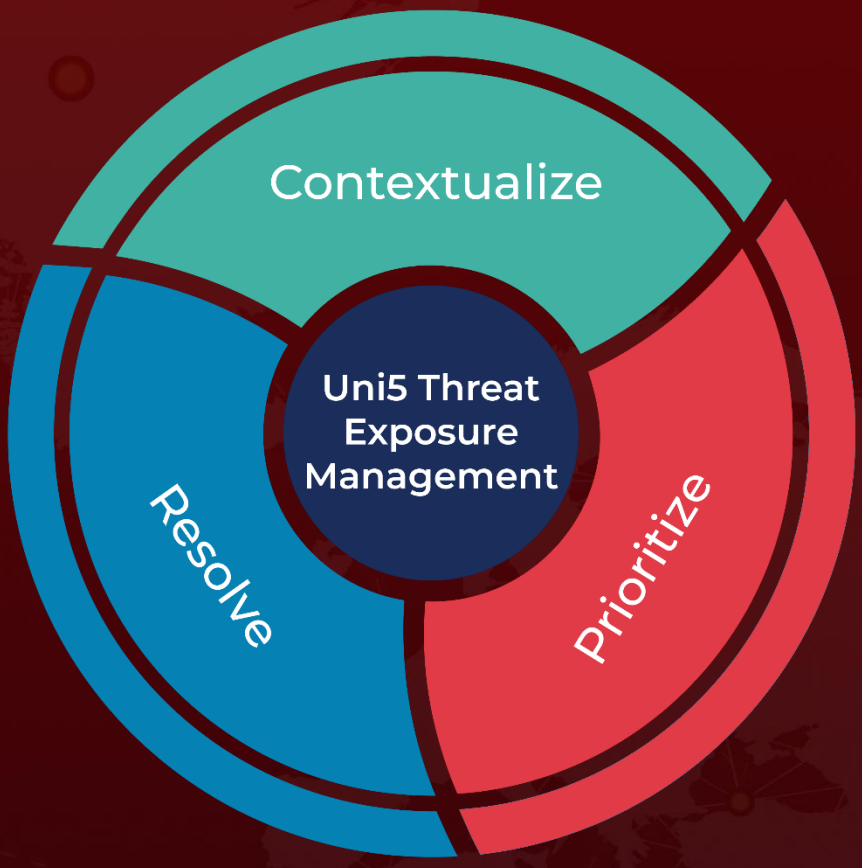
https://hivepro.com/threat-advisory/instant-root-access-via-cve-2026-24061-a-decade-old-bug-comes-alive/

https://hivepro.com/threat-advisory/google-chrome-css-use-after-free-zero-day-vulnerability-cve-2026-2441/

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

February 24, 2026 • 9:00 AM

More at www.hivepro.com