Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

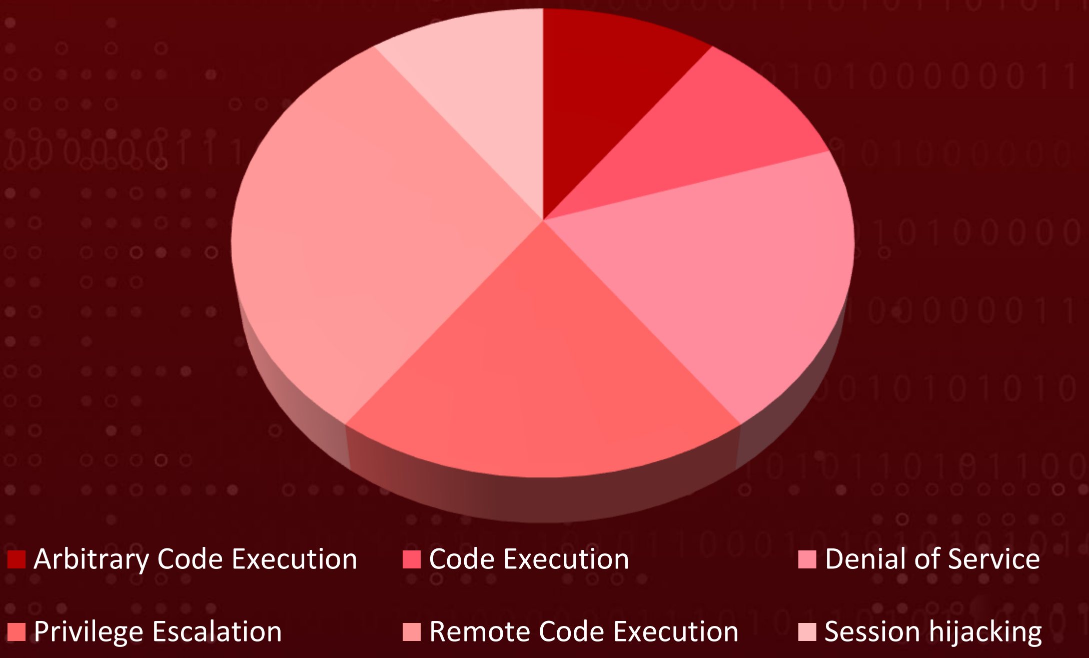
March 2026 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
March 25, 2026	A1	TA2026081

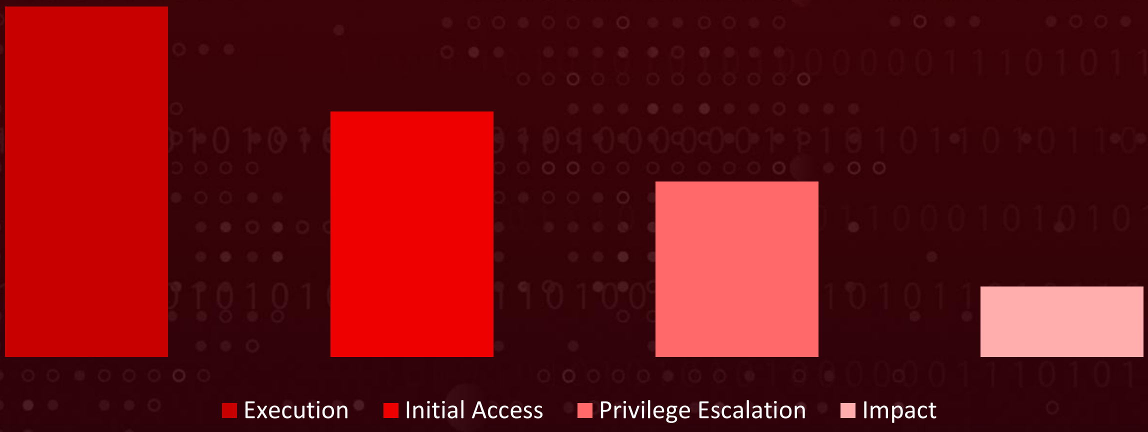
Summary

In March, more than **597** new vulnerabilities were discovered and addressed within the Linux ecosystem, impacting several major distributions such as Debian, SUSE, Ubuntu, and Red Hat. During this period, over **3175** 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 which are exploited or have 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-2025-38352*	Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability	Android Kernel, Linux Kernel, Debian, Ubuntu, SUSE, Oracle, Linux	Privilege Escalation	Local
CVE-2025-68461*	RoundCube Webmail Cross-site Scripting Vulnerability	RoundCube Webmail, Debian, Ubuntu, SUSE, Red Hat	Session hijacking	Network
CVE-2026-21945	Oracle Java SE/ GraalVM Denial of Service Vulnerability	Oracle Java SE/ GraalVM, Debian, Ubuntu, SUSE, Red Hat	Denial of Service	Network
CVE-2026-3909*	Google Skia Out-of-Bounds Write Vulnerability	Google Chrome	Remote Code Execution	Phishing
CVE-2026-3910*	Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability	Google Chrome	Arbitrary Code Execution	Phishing
CVE-2024-26581	Linux Kernel netfilter Race Condition Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE, Red Hat	Privilege Escalation	Local
CVE-2025-11187	OpenSSL Denial of Service Vulnerability	OpenSSL, Debian, Ubuntu, SUSE, Red Hat	Denial of Service	Local

* 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-2025-53367	DjVuLibre Out-of-Bounds Write Vulnerability	DjVuLibre, Ubuntu, RedHat, Debian, SUSE	Code Execution	Local
CVE-2026-22778	vLLM Remote Code Execution Vulnerability	vLLM, Red Hat	Remote Code Execution	Network
CVE-2026-32746	GNU Inetutils telnetd Buffer Overflow Vulnerability	GNU Inetutils telnetd, SUSE, Debian, Ubuntu, Red Hat	Remote Code Execution	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-2025-38352	✗	Android Kernel, Linux Kernel, Debian, Ubuntu, SUSE, Oracle, Linux	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:google:android:-:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:* cpe:2.3:o:oracle:*:*:*:*:*:*:*:*	-
Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-367	T1204: User Execution, T1068: Exploitation for Privilege Escalation	Debian, Ubuntu, SUSE, Oracle, Linux, Android

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-68461	✗	Roundcube Webmail before 1.5.12 and 1.6 before 1.6.12, Debian, Ubuntu, SUSE, Red Hat	APT28, Winter Vivern
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*	-
RoundCube Webmail Cross-site Scripting Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189 : Drive-by Compromise	Roundcube Webmail, Debian, Ubuntu, SUSE, Red Hat

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-3909	✗	Google Chrome (before 146.0.7680.75)	-
	ZERO-DAY	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
	✓	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
NAME	CISA KEV		
Google Skia Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	Google Chrome

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-3910	✗	Google Chrome (before 146.0.7680.75)	-
	ZERO-DAY	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
	✓	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
NAME	CISA KEV		
Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94 CWE-119	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059.007: Command & Scripting Interpreter: JavaScript	Google Chrome

Vulnerability Details

#1

In March, the Linux ecosystem addressed over **3175** vulnerabilities across various distributions and products, covering critical issues such as denial of service, privilege escalation, and remote code execution. Additionally, **597** newly discovered vulnerabilities were patched. HiveForce Lab has identified **10** critical vulnerabilities that are either currently being exploited or highly likely to be targeted soon. Notably, four of these vulnerabilities are under active exploitation, requiring immediate attention and remediation.

#2

Starting with legacy infrastructure threats, CVE-2026-32746 is a critical pre-authentication remote code execution vulnerability (CVSS 9.8) in GNU InetUtils telnetd, a 32-year-old buffer overflow in the LINEMODE SLC handler that allows unauthenticated attackers to achieve root-level code execution over port 23, with multiple public exploits already available. Similarly, CVE-2026-22778, a critical RCE flaw (CVSS 9.8) in vLLM AI inference engine, enables full server compromise through a malicious video URL by chaining an ASLR bypass with a heap buffer overflow.

#3

Browser-based threats remain prominent, with two actively exploited Google Chromium zero-days. CVE-2026-3909 and CVE-2026-3910 affect the Skia graphics library and V8 JavaScript engine respectively, enabling remote code execution through crafted HTML pages and impacting all Chromium-based browsers.

#4

Linux kernel and system-level components continue to be prime targets. CVE-2025-38352, a TOCTOU race condition in the kernel's POSIX CPU timers, saw renewed urgency after the "Chronomaly" exploit demonstrated complete privilege escalation to root on vulnerable 5.10.x kernels. CVE-2024-26581, a netfilter nft_set_rbtree race condition (CVSS 7.8), allows local privilege escalation through improper garbage collection handling.

#5

Critical vulnerabilities in widely-deployed services were also addressed. CVE-2025-68461, a Roundcube Webmail XSS vulnerability, enables silent email account takeover through malicious SVG animate tags. CVE-2026-21945, an Oracle Java SE denial of service flaw (CVSS 7.5), allows unauthenticated remote crashes. CVE-2025-11187, an OpenSSL PKCS#12 stack overflow affecting versions 3.4-3.6, ships alongside the critical CVE-2025-15467 (CVSS 9.8). CVE-2025-53367, a DjVuLibre out-of-bounds write, can lead to code execution when users open crafted documents in default Linux viewers.

#6

March 2026's vulnerability landscape reflects continued high-risk trends, with active exploitation of legacy protocols, kernel flaws, browser engines, and widely-deployed services posing urgent threats. Timely patching and defense-in-depth strategies remain essential to prevent system compromise.

Recommendations

Proactive Strategies:

Exposure Assessment: Conduct a comprehensive service exposure evaluation to identify any publicly accessible services, development hosts, or data processing endpoints that may be vulnerable to exploitation. Prioritize exposure assessment for systems running vLLM AI inference endpoints, Chromium-based browsers, Roundcube Webmail instances, Java/GraalVM deployments, and Linux kernels with NVMe-TCP or netfilter configurations.

Regular Patch Management & Kernel Updates: Ensure all Linux distributions, installed packages, and kernel versions are updated to the latest security patches. Automate updates using tools such as unattended-upgrades, DNF Automatic, or apt-cron to reduce the window of exposure. Pay particular attention to critical updates addressing CVE-2026-32746, CVE-2025-38352, CVE-2026-22778, and the OpenSSL patch bundle including CVE-2025-11187 and CVE-2025-15467.

Disable Legacy Services & Reduce Attack Surface: With CVE-2026-32746 exposing a 32-year-old pre-auth RCE in telnetd, immediately audit all systems for active Telnet services. Disable telnetd wherever possible and migrate to SSH. Block port 23 at the network perimeter. For AI infrastructure, restrict vLLM API endpoints to trusted networks, implement API authentication, and disable multimodal video processing if not business-critical. Enforce SELinux or AppArmor policies to restrict process permissions and prevent privilege escalation.

Harden Browser and Web-Facing Applications: With CVE-2026-3909 and CVE-2026-3910 actively exploited in Chromium, it is imperative to update all browsers, email clients, and web applications to the latest supported versions. For Roundcube Webmail deployments, upgrade to version 1.5.12 or 1.6.12 immediately and implement Content Security Policy headers to mitigate XSS risks.

Reactive Strategies:

Deploy or tighten endpoint detection and response (EDR), SIEM rules, and network traffic analysis to detect exploitation attempts and persistence mechanisms. Focus on Telnet exploitation patterns on port 23, suspicious ptrace-based kernel privilege escalation activity, malformed video URL submissions to AI inference APIs, and browser-related script execution anomalies.

In case of system compromise, immediately isolate it from the network to prevent further spread. Use iptables or nftables to block malicious traffic, revoke credentials of affected users, and restore from a clean, verified backup before reconnecting.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-38352	T1204: User Execution, T1068: Exploitation for Privilege Escalation	DET0478: User Execution – multi-surface behavior chain (documents/links → helper/unpacker → LOLBIN/child → egress) DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software M1017: User Training M1050: Exploit Protection M1038: Execution Prevention	✓ Debain Ubuntu SUSE Oracle Linux
CVE-2025-68461	T1189 : Drive-by Compromise	DET0176: Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189)	M1051: Update Software M1017: User Training M1021: Restrict Web-Based Content	✓ Roundcube Webmail Debian Ubuntu SUSE Red Hat
CVE-2026-21945	T1499: Endpoint Denial of Service, T1190: Exploit Public-Facing Application	DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms, DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)	M1051: Update Software, M1037:Filter Network Traffic, M1038: Execution Prevention	✓ Oracle Debain Ubuntu SUSE Red Hat

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-3909	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	DET0176: Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189) DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software M1017: User Training M1021: Restrict Web-Based Content M1038: Execution Prevention M1050: Exploit Protection	✓ Google Chrome
CVE-2026-3910	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059.007: Command & Scripting Interpreter: JavaScript	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), DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Google Chrome
CVE-2024-26581	T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software M1017: User Training M1038: Execution Prevention M1050: Exploit Protection	✓ Linux Kernel Debian Ubuntu SUSE Red Hat

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-11187	T1499: Endpoint Denial of Service, T1203: Exploitation for Client Execution	DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms, DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1051: Update Software M1017: User Training M1021: Restrict Web-Based Content M1038: Execution Prevention	✓ OpenSSL Debian Ubuntu Red Hat SUSE
CVE-2025-53367	T1204: User Execution, T1203: Exploitation for Client Execution	DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0478: User Execution – multi-surface behavior chain (documents/links → helper/unpacker → LOLBIN/child → egress)	M1038: Execution Prevention M1050: Exploit Protection Content M1017: User Training	✓ DjVuLibre Red Hat Ubuntu SUSE Debian
CVE-2026-22778	T1190: Exploit Public-Facing Application, 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)	M1051: Update Software M1017: User Training M1021: Restrict Web-Based Content	✓ vLLM Red Hat

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-32746	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	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) DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software M1017: User Training M1038: Execution Prevention M1050: Exploit Protection	✓ SUSE ✗ GNU Inetutils Telnetd Debian Ubuntu Red Hat

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/

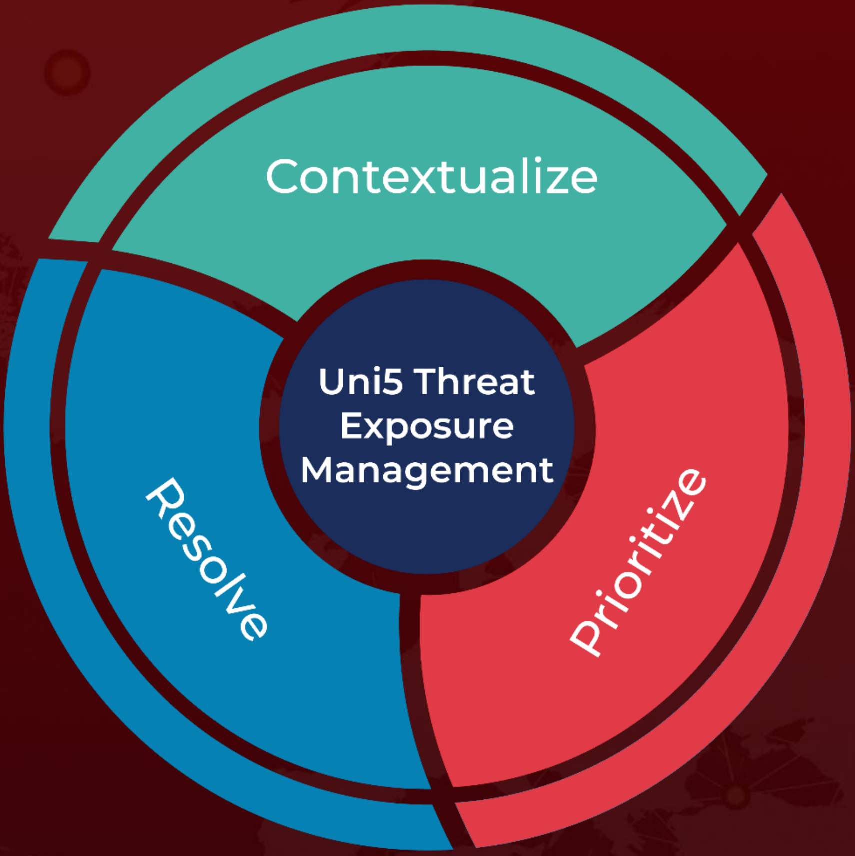
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/

https://hivepro.com/threat-advisory/google-rushes-to-fix-actively-exploited-flaws/

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

March 25, 2026 • 02:15 AM

More at www.hivepro.com