Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

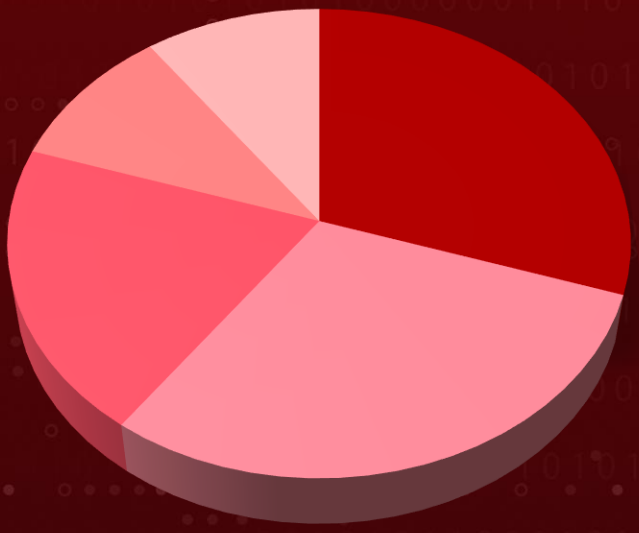
December 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
December 26, 2025	A1	TA2025389

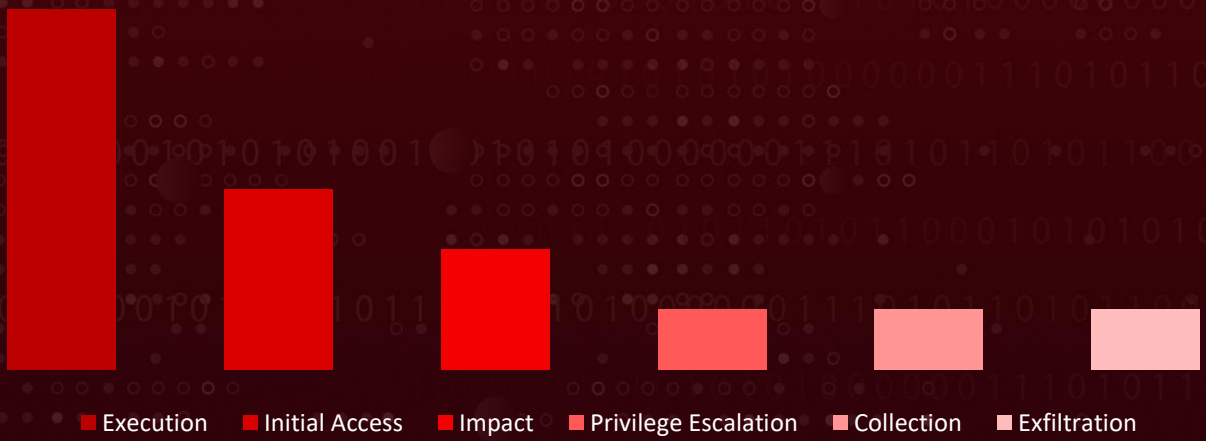
Summary

In December, more than **1700** 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 **2390** 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-2025-43529*	Apple Multiple Products Use-After-Free WebKit Vulnerability	Apple Multiple Products	Arbitrary Code Execution	Network
CVE-2025-14174*	Google Chromium Out of Bounds Memory Access Vulnerability	Google Chromium	Arbitrary Code Execution	Network
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-2023-44487*	HTTP/2 Rapid Reset Attack Vulnerability	IETF HTTP/2, Debian, Red Hat, Ubuntu	Denial of Service	Network
CVE-2023-48022*	Anyscale Ray Remote Code Execution Vulnerability	Anyscale Ray	Remote Code Execution	Network
CVE-2024-4741	Openssl Use-After-Free Vulnerability	OpenSSL, Ubuntu, RedHat, Debian, SUSE, Amazon Linux, Oracle	Code Execution	Network
CVE-2025-49844*	RediShell (Redis Remote Code Execution Vulnerability)	Ubuntu, Red Hat, Debian, SUSE, Redis	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.

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-41115	Grafana Enterprise SCIM Privilege Escalation Vulnerability	Grafana Enterprise SCIM	Privilege Escalation	Network
CVE-2025-66516	Apache Tika XXE Injection Vulnerability	Apache Tika	Information Disclosure	Network
CVE-2022-0778	OpenSSL Infinite Loop Vulnerability	OpenSSL	Denial of Service	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-2025-43529	✗	Apple Multiple Products, Debain, Ubuntu, SUSE, Oracle, Red Hat	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:* cpe:2.3:o:oracle:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:*	-
Apple Multiple Products Use-After-Free WebKit Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	Apple, Ubuntu, RedHat, Debian, SUSE, Oracle

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-14174		Google Chrome prior 143.0.7499.109 (Linux), Safari: versions earlier than 26.2, Microsoft Edge (macOS): versions prior to 143.0.3650.80	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*:*	-
Google Chromium Out of Bounds Memory Access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119 CWE-787	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	Google Chrome, Microsoft Edge

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 PRODUCTS	ASSOCIATED ACTOR
CVE-2023-44487	✗	Debian, Red Hat, Ubuntu	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:*	-
HTTP/2 Rapid Reset Attack Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-400	T1588: Obtain Capabilities, T1498: Network Denial of Service, T1584: Compromise Infrastructure	Debian, Red Hat, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-48022	✗	Anyscale Ray 2.6.3 and 2.8.0, Ubuntu, RedHat, Debian	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:anyscale:ray:2.6.3:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:*	XMRig
Anyscale Ray Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1190 : Exploit Public-Facing Application, T1203 : Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	Ubuntu, RedHat, Debian No official patch - vendor (Anyscale Ray)

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49844	RediShell	All Versions of Redis with Lua Scripting (Before 8.2.2), Ubuntu, Red Hat, Debian, SUSE	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redis:redis:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:* cpe:2.3:o:suse:suse:-:*:*:*:*:*:*:*	-
Redis Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion	Ubuntu, Red Hat, Debian, SUSE, Redis

Vulnerability Details

#1

In December, the Linux ecosystem addressed over **2390** vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and remote code execution. Additionally, **1700** 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, six of these vulnerabilities are under active exploitation, requiring immediate attention and remediation.

#2

Starting with browser-based threats, CVE-2025-14174 is a zero-day vulnerability in Google Chrome's ANGLE graphics library that allows remote code execution through maliciously crafted web content and has been actively exploited in the wild. Similarly, CVE-2025-43529 affects Apple WebKit where a use-after-free vulnerability enables arbitrary code execution through malicious web content, representing a significant cross-platform threat.

#3

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, allows local privilege escalation through use-after-free memory corruption, primarily affecting 32-bit Android and Linux devices. CVE-2022-0778, an OpenSSL infinite loop vulnerability triggered by malformed X.509 certificates, causes denial of service through CPU exhaustion on TLS-enabled services.

#4

Critical vulnerabilities in widely-deployed services were also addressed. CVE-2025-49844, dubbed "RediShell," is a maximum-severity flaw in Redis allowing authenticated attackers to achieve remote code execution via malicious Lua scripts. CVE-2025-66516, a critical XXE injection in Apache Tika, enables attackers to access sensitive resources through malicious PDFs. Additionally, CVE-2023-44487, the HTTP/2 Rapid Reset attack, continues to impact web infrastructure by enabling massive DDoS attacks through rapid request-cancellation sequences.

#5

December 2025's vulnerability landscape reflects continued high-risk trends, with active exploitation of 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 affected Linux kernels, Redis instances, Apache Tika servers, Grafana dashboards, Chrome browsers, and HTTP/2-enabled web servers.

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-2025-49844, CVE-2025-38352, and other kernel-level vulnerabilities.

Harden Browser and Web-Facing Applications: With CVE-2025-14174 actively exploited in Chrome, it is imperative to update all browsers, email clients, and web applications to the latest supported versions. Enable automatic updates where possible and enforce secure configurations to mitigate remote code execution risks. Consider disabling outdated or unsupported plugins, enforcing site isolation, and monitoring browser telemetry for anomalous activity linked to web-based exploits.

Access Control & Least Privilege Implementation: Enforce SELinux or AppArmor policies to restrict process permissions and prevent privilege escalation. Implement sudo with least privilege access, disable unnecessary services, and restrict root login to reduce attack surfaces. For Grafana Enterprise deployments, immediately patch CVE-2025-41115 and audit SCIM provisioning configurations.

Reactive Strategies:

Deploy or tighten endpoint detection and response (EDR), SIEM rules, and network traffic analysis to detect late-stage exploitation attempts or persistence mechanisms. Focus on Redis command injection patterns, HTTP/2 rapid reset anomalies, 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 and revoke credentials of affected users. Restore from a clean, verified backup to ensure system integrity before reconnecting to the network.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-43529	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software M1021: Restrict Web-Based Content	Google Chrome Ubuntu RedHat Debian SUSE Oracle
CVE-2025-14174	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	Google Chrome Apple Microsoft Edge
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 ID	TTPs	Detection	Mitigation	Patch
CVE-2023-44487	T1588: Obtain Capabilities, T1498: Network Denial of Service, T1584: Compromise Infrastructure	DET0518: Behavioral Detection of T1498 – Network Denial of Service Across Platforms, DET0885:Detection of Compromise Infrastructure	M1037: Filter Network Traffic M1056: Pre-compromise	Debian Red Hat Ubuntu
CVE-2023-48022	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	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	Red Hat Ubuntu RedHat Debian
CVE-2024-4741	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	OpenSSL Ubuntu RedHat Debian SUSE Amazon Linux Oracle Linux
CVE-2025-49844*	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion	DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse, DET0046: Detection Strategy for T1497 Virtualization/Sandbox Evasion	M1038: Execution Prevention, M1026: Privileged Account Management, M1033: Limit Software Installation, M1040: Behavior Prevention on Endpoint	Ubuntu Red Hat Debian SUSE Redis

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-41115	T1190: Exploit Public-Facing Application, T1078: Valid Accounts, T1136: Create Account	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0560: Detection of Valid Account Abuse Across Platforms	M1038: Execution Prevention M1051: Update Software M1017: User Training	✓ Grafana Debian Ubuntu SUSE Red Hat
CVE-2025-66516	T1190: Exploit Public-Facing Application, T1005: Data from Local System	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0380: Detection of Local Data Collection Prior to Exfiltration	M1017: User Training M1045: Code Signing M1051: Update Software, M1057: Data Loss Prevention	✓ Apache Tika Red Hat ✗ Debian, Ubuntu,
CVE-2022-0778	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1190: Exploit Public-Facing Application	DET0518: Behavioral Detection of T1498 – Network Denial of Service 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	✓ OpenSSL Debian Ubuntu SUSE Red Hat Oracle

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/

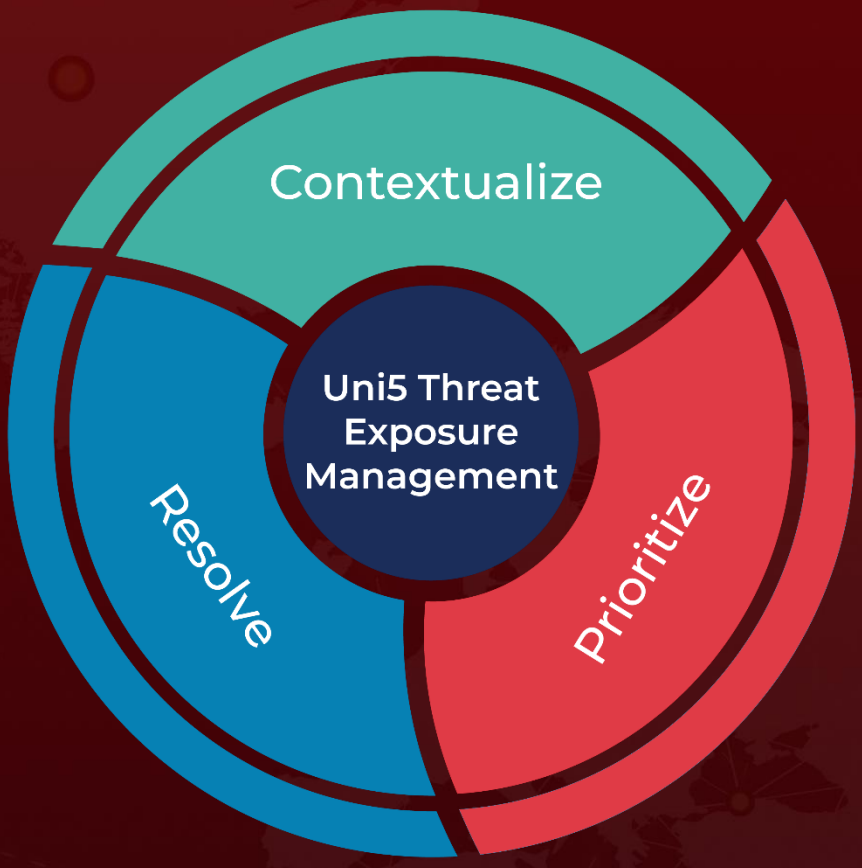
https://hivepro.com/threat-advisory/shadowray-strikes-back-inside-the-multi-purpose-ray-cluster-takeover/

https://hivepro.com/threat-advisory/openssl-exposed-to-denial-of-service-vulnerability-causing-infinite-loop/

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

December 26, 2025 . 1:30 AM

More at www.hivepro.com