Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

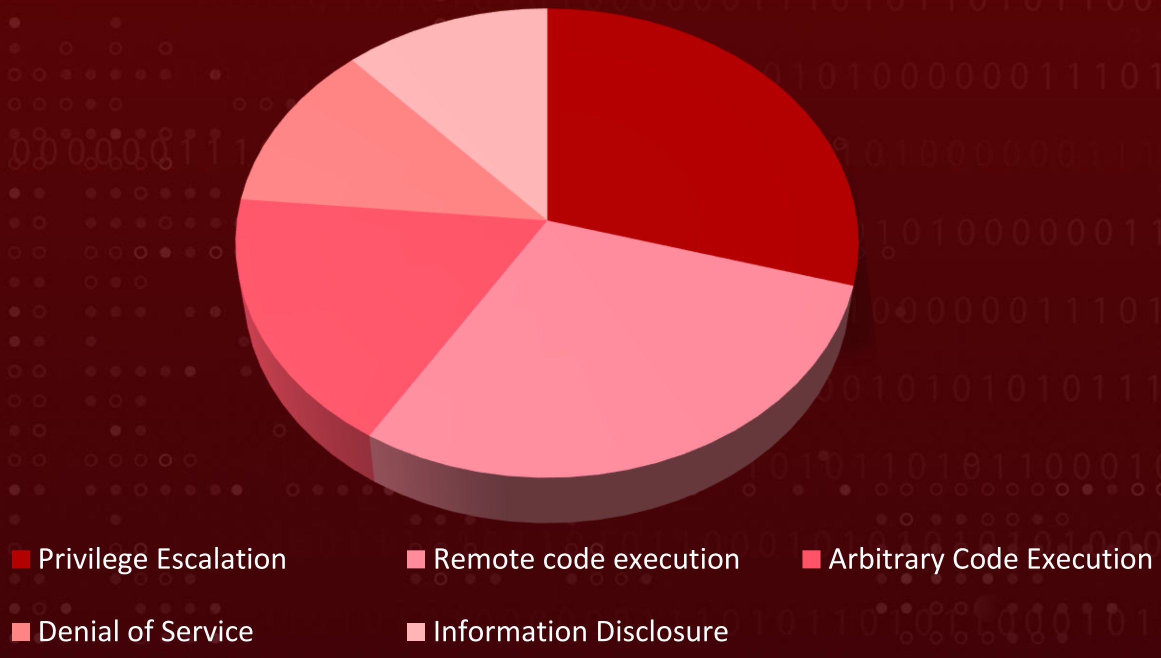
September 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
September 26, 2025	A1	TA2025298

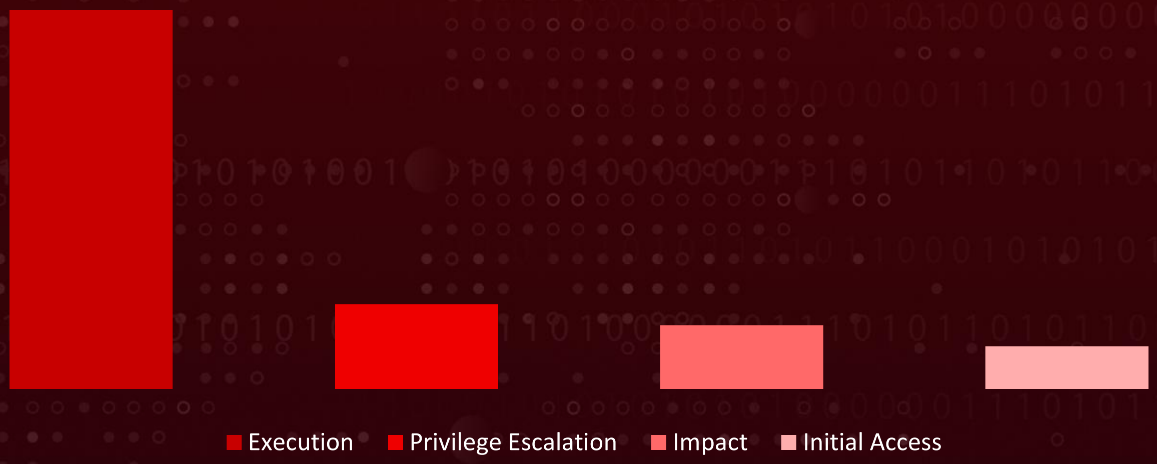
Summary

In September, more than **1348** 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 **2151** 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 **13** 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-2021-0920*	Android Kernel Race Condition Vulnerability	Android Kernel, Linux Kernel, Debain, Ubuntu, SUSE, Oracle, Red Hat	Privilege Escalation	Local
CVE-2025-10585*	Google Chromium V8 Type Confusion 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, Debain, Ubuntu, SUSE, Oracle	Privilege Escalation	Local
CVE-2025-48384*	Git Link Following Vulnerability	Git Link, Debain, Ubuntu, SUSE, Oracle	Arbitrary code execution	Network
CVE-2025-54574	Squid Heap Buffer Overflow Vulnerability	Squid, Debian, Ubuntu, SUSE	Remote code execution	Remote
CVE-2025-57833	Django SQL injection Vulnerability	Django, Debian, Ubuntu, SUSE	Remote Code Execution	Remote
CVE-2025-59359	Chaos Mesh OS Command Injection Vulnerability	Chaos Mesh (Chaos Controller Manager Component), SUSE	Privilege Escalation	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-2025-8067	Linux UDisks daemon Out-of-bounds Read Vulnerability	Linux UDisks daemon, Debian, Ubuntu, SUSE, Oracle Linux, Red Hat	Privilege Escalation	Local
CVE-2025-8714	PostgreSQL Arbitrary Code Execution Vulnerability	PostgreSQL, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Amazon Linux, Oracle Linux	Arbitrary Code Execution	Network
CVE-2025-59360	Chaos Mesh OS Command Injection Vulnerability	Chaos Mesh (Chaos Controller Manager Component), SUSE	Remote Code Execution	Remote
CVE-2025-59361	Chaos Mesh OS Command Injection Vulnerability	Chaos Mesh (Chaos Controller Manager Component), SUSE	Remote Code Execution	Network
CVE-2025-27466	Xen NULL Pointer Dereference Vulnerability	Xen, Red Hat, Debian, Ubuntu	Denial of Service, Privilege Escalation, Information Disclosure	Network
CVE-2025-57052	cJSON library Out-of-bounds Access Vulnerability	cJSON library, Debian, Ubuntu, SUSE, Red Hat	Denial of Service, Remote Code Execution, Information Disclosure	Remote

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-2021-0920	✗	Android Kernel, Linux Kernel, Debain, Ubuntu, SUSE, Oracle, Red Hat	-
	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:redhat:*:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:* cpe:2.3:o:oracle:*:*:*:*:*:*:*:*	-
Android Kernel Race Condition Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-362 CWE-416	T1204: User Execution, T1068: Exploitation for Privilege Escalation	Andriod, Debain, Ubuntu, SUSE, Oracle, Red Hat

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-10585	✗	Google Chromium V8, Microsoft Edge	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1189: Drive-by Compromise, T1059.007 Command and Scripting Interpreter: JavaScript, T1203: Exploitation for Client Execution	Google Chrome, Microsoft Edge

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-38352	✗	Android Kernel, Linux Kernel, Debain, 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	Debain, Ubuntu, SUSE, Oracle, Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-48384	✗	Git Link, Debain, Ubuntu, SUSE, Oracle	Lazarus Group
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:git-scm:git:*:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:*:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:*	-
Git Link Following Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-436 CWE-59	T1204: User Execution, T1059: Command and Scripting Interpreter	Git Link, Debain, Ubuntu, SUSE, Oracle

Vulnerability Details

#1

In September, the Linux ecosystem addressed over **2151** vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and remote code execution. Additionally, **1348** newly discovered vulnerabilities were patched. HiveForce Lab has identified **13** critical vulnerabilities that are either currently being exploited or highly likely to be targeted soon.

#2

These vulnerabilities facilitate adversarial tactics such as Initial Access, Execution, Privilege Escalation, and Impact. Notably, four of these vulnerabilities are under active exploitation, requiring immediate attention and remediation.

#3

Starting with Google Chrome, the most critical fix is **CVE-2025-10585**, a zero-day vulnerability in the V8 JavaScript engine. This flaw allows remote code execution through crafted web pages and has been actively exploited.

#4

Linux kernel and system-level components were also impacted. CVE-2021-0920, a race condition in Android and Linux kernels that allows local privilege escalation through the Unix domain socket subsystem. CVE-2025-38352 is a TOCTOU race in the kernel's POSIX CPU timers, allowing local escalation of privileges, while CVE-2025-48384, actively exploited by the Lazarus group, allows arbitrary file writes through malicious Git submodules, creating a high-risk attack vector for developers and CI/CD pipelines.

#5

Additional critical vulnerabilities patched include CVE-2025-54574, a heap buffer overflow in Squid that could allow remote code execution via URN processing, and , a Chaos Mesh OS command injection enabling remote code execution in cluster environments. Other vulnerabilities such as CVE-2025-8067 (UDisks daemon), CVE-2025-8714 (PostgreSQL), and vulnerabilities including CVE-2025-27466 and CVE-2025-57052 expose systems to privilege escalation, denial-of-service, or information disclosure if left unpatched.

#6

September 2025's vulnerability landscape reflects a continuation of high-risk trends in the Linux ecosystem, with active kernel and developer-tool exploits posing the most urgent threats. The nature of these issues ranges from local privilege escalation to potential denial-of-service conditions, underscoring the importance of timely patching and mitigation to prevent potential system compromise.

Recommendations

Proactive Strategies:

Exposure Assessment: Conduct a comprehensive service exposure evaluation to identify any publicly accessible services, development hosts, or CI/CD endpoints that may be vulnerable to exploitation. Prioritize exposure assessment for systems running affected Linux kernels, Git clients, Chrome browsers, Squid proxies, PostgreSQL instances, and Chaos Mesh controllers. Any identified vulnerabilities should be remediated immediately through patching or configuration adjustments to reduce the attack surface.

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-2021-0920, CVE-2025-38352, and other kernel-level vulnerabilities that could allow privilege escalation or denial-of-service attacks.

Harden Browser and Web-Facing Applications: With CVE-2025-10585 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.

Review and Secure Software Dependencies: Development environments and CI/CD pipelines must ensure that all software dependencies, including Python libraries, HTTP parsers, cryptographic components, and Git clients, are current and free of known vulnerabilities.

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.

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 web, browser, and script-related 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-2021-0920	T1204: User Execution T1068: Exploitation for Privilege Escalation	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software M1017: User Training M1050: Exploit Protection	✓ Debain, Ubuntu, SUSE, Oracle, Red Hat, Andriod
CVE-2025-10585	T1189: Drive-by Compromise T1059.007 Command and Scripting Interpreter: JavaScript T1203: Exploitation for Client Execution	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Google Chrome, Microsoft Edge, Chromium
CVE-2025-38352	T1204: User Execution T1068: Exploitation for Privilege Escalation	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software M1017: User Training M1050: Exploit Protection	✓ Debain, Ubuntu, SUSE, Oracle, Linux
CVE-2025-48384	T1204: User Execution T1059: Command and Scripting Interpreter	DS0009: Process DS0017: Command Execution	M1038: Execution Prevention M1017: User Training	✓ Git Link, Debain, Ubuntu, SUSE, Oracle
CVE-2025-54574	T1203: Exploitation for Client Execution T1059: Command and Scripting Interpreter T1210: Exploitation of Remote Services	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Squid, Debian, Ubuntu, SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-57833	T1059: Command and Scripting Interpreter	DS0009: Process DS0017: Command Execution	M1038: Execution Prevention	✓ Django, Debian, Ubuntu, SUSE
CVE-2025-59359	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter T1068: Exploitation for Privilege Escalation	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Chaos Mesh, SUSE
CVE-2025-8067	T1068: Exploitation for Privilege Escalation T1499: Endpoint Denial of Service	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1037:Filter Network Traffic	✓ Udisks, Debian, Ubuntu, SUSE, Oracle, Red Hat
CVE-2025-8714	T1204.002: User Execution: Malicious File T1059: Command and Scripting Interpreter	DS0009: Process DS0017: Command Execution	M1017: User Training M1050: Exploit Protection	✓ PostgreSQL, Debian, Ubuntu, SUSE, Oracle, Red Hat
CVE-2025-59360	T1059: Command and Scripting Interpreter T1203: Exploitation for Client Execution	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1051: Update Software	✓ Chaos Mesh, SUSE
CVE-2025-59361	T1059: Command and Scripting Interpreter T1203: Exploitation for Client Execution	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1051: Update Software	✓ Chaos Mesh, SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-27466	T1068: Exploitation for Privilege Escalation T1499: Endpoint Denial of Service	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1037:Filter Network Traffic	✓ Xen, Red Hat ✗ Debian, Ubuntu
CVE-2025-57052	T1203: Exploitation for Client Execution T1499: Endpoint Denial of Service	DS0009: Process DS0022: File Modification DS0029: Network Traffic	M1051: Update Software M1038: Execution Prevention M1037:Filter Network Traffic	✓ Debian ✗ Ubuntu, SUSE, 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/

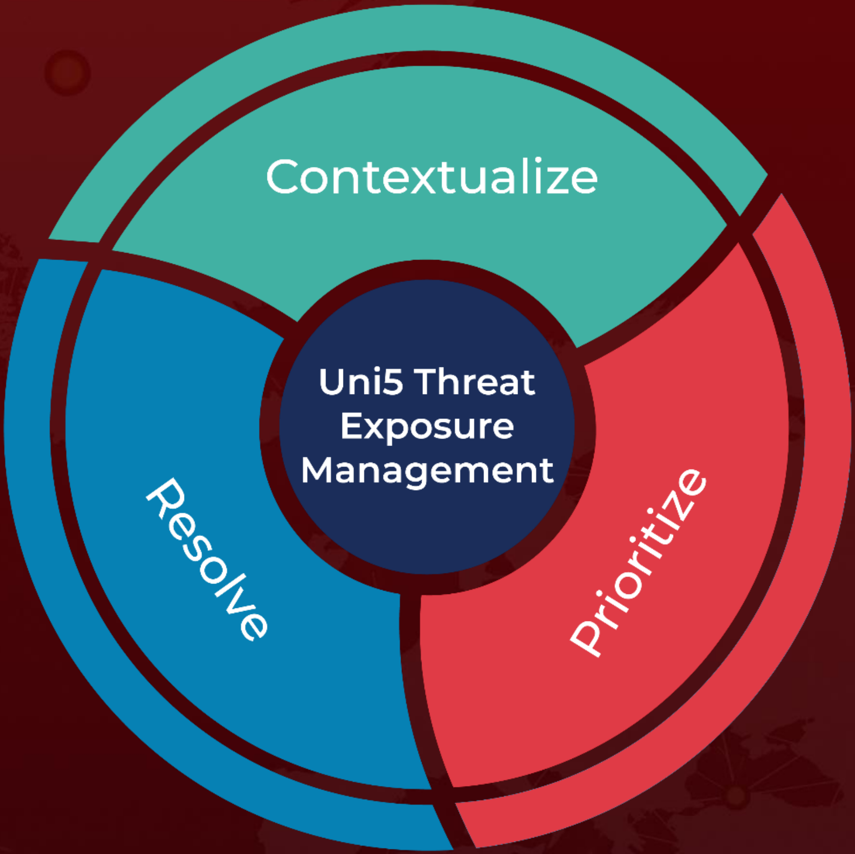
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/

https://hivepro.com/threat-advisory/google-races-to-patch-chrome-sixth-zero-day-cve-2025-10585/

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

September 26, 2025 • 10:30 AM

More at www.hivepro.com