

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

November 2025 Linux Patch Roundup

Date of Publication

November 24, 2025

Admiralty Code

A1

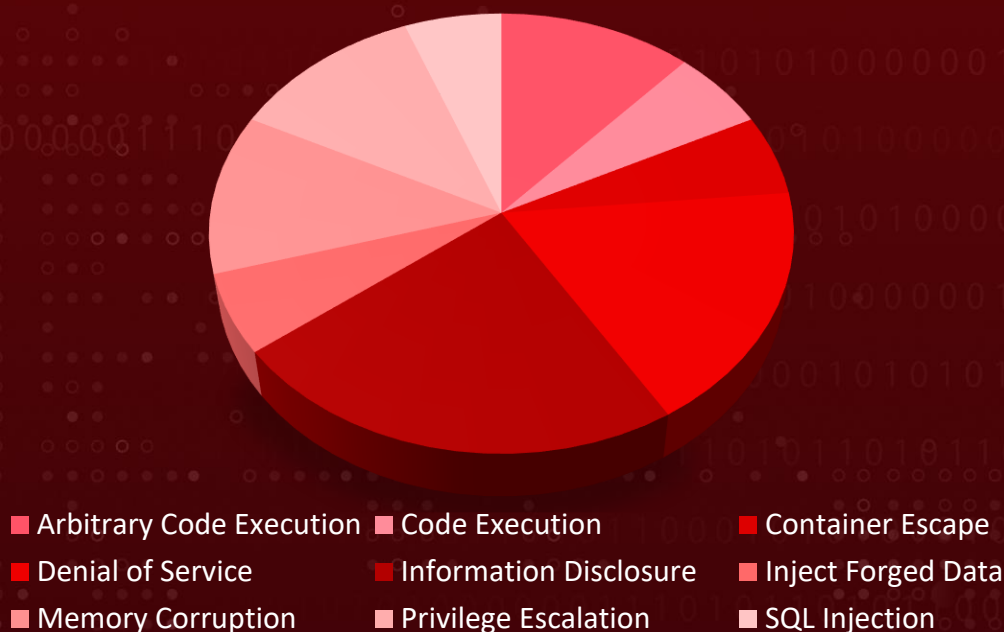
TA Number

TA2025357

Summary

In **November**, more than **1384** new vulnerabilities were discovered and addressed within the Linux ecosystem, impacting several major distributions such as Debian, Red Hat, OpenSUSE, and Ubuntu. During this period, over **2692** 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** 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-2024-50302*	Linux Kernel Use of Uninitialized Resource Vulnerability	Linux Kernel, Red Hat Enterprise Linux CoreOS (RHCOS), Debian, Ubuntu, SUSE, Amazon Linux, Oracle Linux	Information Disclosure	Local
CVE-2024-53104*	Linux Kernel Out-of-Bounds Write Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE, ALT Linux, Red Hat	Information Disclosure	Local
CVE-2024-53150*	Linux Kernel Out-of-Bounds Read Vulnerability	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	Information Disclosure	Local
CVE-2024-53197*	Linux Kernel Out-of-Bounds Access Vulnerability	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	Privilege Escalation	Local
<u>CVE-2025-13223*</u>	Google Chromium V8 Type Confusion Vulnerability	Google Chromium	Memory Corruption	Network
CVE-2025-40778	BIND 9 Cache Poisoning via Unsolicited Answer Records Vulnerability	Ubuntu, Red Hat, Amazon, Suse, Debian, Oracle	Inject Forged Data	Network
CVE-2025-52565	runc Insufficient Validation Vulnerability	Ubuntu, Suse, Amazon, Debian, Red Hat, Oracle	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-2025-31133	runc maskedPaths feature Bypass Vulnerability	Ubuntu, Suse, Amazon, Debian, Red Hat, Oracle	Information Disclosure, Denial of Service	Local
CVE-2025-52881	runc Racing Container Vulnerability	Ubuntu, Suse, Amazon, Debian, Red Hat, Oracle	Container Escape, Denial of Service, Privilege Escalation	Local
CVE-2025-57108	Kitware VTK Heap Use-after-free Vulnerability	Debian	Arbitrary Code Execution, Memory Corruption	Network
CVE-2025-64459	Django SQL Injection Vulnerability	Ubuntu, Suse, Debian	SQL Injection	Network
CVE-2025-47151	Lasso SAML Library Type Confusion Vulnerability	Ubuntu, Suse, Amazon, Debian, Red Hat, Oracle	Arbitrary Code Execution	Network
CVE-2025-55754	Apache Tomcat Improper Neutralization Vulnerability	Suse, Debian, Red Hat	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-2024-50302		Linux Kernels before 5.4.286, Kernels before 4.19.324, Kernels before 5.10.230, Kernels before 5.15.172, Kernels before 6.1.117, Kernels before 6.6.61, Kernels before 6.11.8, Ubuntu, Suse, Debian, Oracle, Red Hat, Amazon	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Linux Kernel Use of Uninitialized Resource Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-908	T1499: Endpoint Denial of Service; T1574: Hijack Execution Flow	Linux Kernel , Red Hat , Debian , Ubuntu , SUSE , Amazon Linux , Oracle Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53104		Linux Kernel, Ubuntu, Suse, Debian	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* cpe:2.3:o:ubuntu:ubuntu:*:*:*:*:*:* cpe:2.3:o:suse:*:*:*:*:*:*:* cpe:2.3:o:opensuse:leap:*:*:*:* cpe:2.3:o:fedoraproject:fedora:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1204: User Execution T1068: Exploitation for Privilege Escalation	Debian , Fedora , RedHat , Ubuntu , macOS

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53150		Linux Kernel, Debian, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:* cpe:2.3:o:ubuntu:ubuntu:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-125	T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow	Linux Kernel, Ubuntu, Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53197		Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:* cpe:2.3:o:ubuntu:ubuntu:*:*:*:*:*:* cpe:2.3:o:suse:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Access Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow	Linux Kernel, Ubuntu, RedHat, SUSE, Oracle Linux, Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-13223</u>		Google Chrome prior to 142.0.7444.175	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	<u>Google Chrome</u>

Vulnerability Details

#1

In November, the Linux ecosystem underwent a sweeping wave of security fixes, addressing thousands of vulnerabilities across major distributions and related products. These patches covered a wide range of high-impact issues, spanning information disclosure, privilege escalation, and even code execution. In total, more than **1384** newly discovered flaws were identified and patched. From this broader pool, HiveForce Labs spotlighted 13 vulnerabilities that are already being exploited or are considered highly likely to be weaponised soon.

#2

These weaknesses open the door for attackers to carry out dangerous tactics such as execution and privilege escalation. A few are currently under active exploitation, reinforcing the need for rapid mitigation before they evolve into widespread compromises.

#3

Among the most concerning issues are several Linux Kernel vulnerabilities. CVE-2024-50302 originates from an uninitialized resource in the HID subsystem, potentially leaking kernel memory. Multiple USB-related kernel flaws were also patched, including CVE-2024-53104 (out-of-bounds write in the UVC driver enabling physical privilege escalation), CVE-2024-53150 (out-of-bounds read in USB-audio driver leaking sensitive data), and CVE-2024-53197 (out-of-bounds access via malicious USB devices to manipulate memory, escalate privileges, or execute code). Recent Linux flavours have now released patches addressing all of these issues.

#4

Beyond the kernel, critical weaknesses were found in other high-impact components. CVE-2025-13223, a type confusion bug in Google Chromium's V8 engine, allows heap corruption, a common path to remote code execution.

#5

Another significant flaw, CVE-2025-47151, was discovered in Entr'ouvert Lasso versions 2.5.1 and 2.8.2, an essential SAML library supporting Single Sign-On (SSO). Reported in May 2025 and publicly disclosed in November, this vulnerability stems from a type confusion issue in `lassoNodeImplInitFromXml`, enabling arbitrary code execution and putting authentication architectures at risk.

#6

A critical-severity issue was also found in Apache Tomcat. CVE-2025-55754 involves improper handling of ANSI escape sequences in log messages, which can let attackers manipulate console output or trick administrators into executing harmful commands.

#7

Finally, a critical SQL injection vulnerability (CVE-2025-64459) was uncovered in Django's ORM layer due to unsafe handling of the `_connector` parameter in the `Q` class constructor, giving attackers the ability to craft malicious SQL queries and compromise backend databases.

#8

In summary, while the Linux ecosystem and associated technologies have made strong progress in patching these flaws, organisations must stay vigilant, prioritise updates, and reinforce security hygiene to stay ahead of emerging threats.

Recommendations

Proactive Strategies:



Prioritise Patch Management: Stay on top of security updates, especially for the Linux kernel, Django, Chromium, Tomcat, and SAML libraries. Applying patches quickly drastically reduces the attack surface and keeps known exploits from becoming real incidents.



Strengthen Endpoint and USB Security: Since several vulnerabilities involve USB drivers, restrict the use of untrusted USB devices. Enforce physical security rules, disable unused USB ports where possible, and use endpoint protection to flag suspicious device behavior.



Harden Authentication Systems: Flaws in SSO and SAML components highlight the importance of secure identity infrastructure. Regularly review SSO configurations, rotate secrets, and ensure that SAML libraries and dependencies are always up to date.



Improve Code and Dependency Hygiene: For teams managing web applications, treat third-party libraries as part of your threat surface. Track dependency updates, use automated scanners, and avoid outdated components in production environments.



Implement Least Privilege Everywhere: Make it harder for attackers to escalate privileges by limiting what each user, service, or process can access. Even a kernel or application flaw becomes less dangerous when permissions are tightly controlled.

Reactive Strategies:



Quickly Isolate and Contain the Impact: The moment you suspect exploitation, whether it's a kernel privilege escalation, malicious USB activity, or suspicious SQL behaviour, immediately isolate the affected system. Disconnect it from the network, block risky processes, and stop any ongoing activity. This fast containment step is crucial to prevent attackers from spreading deeper into your environment or compromising additional systems.









Investigate, Patch, and Restore Safely: After containment, begin a focused investigation to confirm how the vulnerability was exploited and what level of access the attacker achieved. Review system logs, check for privilege abuse, memory manipulation, or database tampering, and apply all missing patches, especially for the Linux kernel, Django ORM, Tomcat, Chrome V8, or SAML libraries.



Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-50302*	T1499: Endpoint Denial of Service T1574: Hijack Execution Flow	DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms	M1037: Filter Network Traffic	<div><div>✓</div><div>✗</div><div>Linux Kernel Red Hat Enterprise Linux CoreOS (RHCOS) Ubuntu SUSE Amazon Linux Oracle Linux Debian</div></div>
CVE-2024-53104*	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	<div><div>✓</div><div>✗</div><div>Ubuntu, SUSE, ALT Linux, Red Hat Debian</div></div>
CVE-2024-53150*	T1068: Exploitation for Privilege Escalation T1574: Hijack Execution Flow	DET0514: Detection Strategy for Exploitation for Privilege Escalation , DET0218: Detection Strategy for Hijack Execution Flow across OS platforms	M1038: Execution Prevention M1050: Exploit Protection	<div><div>✓</div><div>✗</div><div>Linux Kernel, Ubuntu, RedHat, SUSE, Oracle Linux Debian</div></div>
CVE-2024-53197*	T1068: Exploitation for Privilege Escalation T1574: Hijack Execution Flow	DET0514: Detection Strategy for Exploitation for Privilege Escalation , DET0218: Detection Strategy for Hijack Execution Flow across OS platforms	M1038: Execution Prevention M1050: Exploit Protection	<div><div>✓</div><div>✗</div><div>Linux Kernel Ubuntu RedHat SUSE Oracle Linux Debian</div></div>

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-13223*	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	<u>DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse</u> , <u>DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)</u>	<u>M1045: Code Signing</u> <u>M1051: Update Software</u>	 <u>Google Chromium</u>
CVE-2025-40778	T1557: Adversary-in-the-Middle	<u>DET0296: Detect Adversary-in-the-Middle via Network and Configuration Anomalies</u>	<u>M1030: Network Segmentation</u>	 <u>Ubuntu, Red Hat, Oracle,</u>  <u>Amazon</u>
CVE-2025-52565	T1498: Network Denial of Service	<u>DET0518: Behavioral Detection of T1498 – Network Denial of Service Across Platforms</u>	<u>M1037: Filter Network Traffic,</u> <u>M1048: Application Isolation and Sandboxing</u>	 <u>Ubuntu, Suse, Amazon, Red Hat, Oracle,</u>  <u>Debian</u>
CVE-2025-31133	T1498: Network Denial of Service, T1068: Exploitation for Privilege Escalation	<u>DET0518: Behavioral Detection of T1498 – Network Denial of Service Across Platforms</u> , <u>DET0514: Detection Strategy for Exploitation for Privilege Escalation</u>	<u>M1037: Filter Network Traffic,</u> <u>M1048: Application Isolation and Sandboxing,</u> <u>M1038: Execution Prevention</u>	 <u>Ubuntu, Suse, Amazon, Red Hat, Oracle,</u>  <u>Debian</u>
CVE-2025-52881	T1498: Network Denial of Service, T1068: Exploitation for Privilege Escalation	<u>DET0518: Behavioral Detection of T1498 – Network Denial of Service Across Platforms</u> , <u>DET0514: Detection Strategy for Exploitation for Privilege Escalation</u>	<u>M1037: Filter Network Traffic,</u> <u>M1048: Application Isolation and Sandboxing,</u> <u>M1038: Execution Prevention</u>	 <u>Ubuntu, Suse, Amazon, Red Hat, Oracle,</u>  <u>Debian</u>
CVE-2025-57108	T1059: Command and Scripting Interpreter	<u>DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse</u>	<u>M1045: Code Signing</u>	 <u>Debian</u>

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-64459	T1055: Process Injection	<u>DET0508: Behavioral Detection of Process Injection Across Platforms</u>	<u>M1026: Privileged Account Management</u>	<div>  <u>Ubuntu, Suse,</u> </div> <div>  <u>Debian</u> </div>
CVE-2025-47151	T1059: Command and Scripting Interpreter	<u>DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse</u>	<u>M1045: Code Signing</u>	<div>  <u>Ubuntu, Suse, Amazon, Red Hat, Oracle,</u> </div> <div>  <u>Debian</u> </div>
CVE-2025-55754	T1566: Phishing, T1059: Command and Scripting Interpreter	<u>DET0070: Detection Strategy for Phishing across platforms</u>	<u>M1017: User Training</u>	<div>  <u>Suse, Red Hat</u> </div> <div>  <u>Debian</u> </div>

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-patches-high-risk-v8-zero-day-hitting-chrome-users/>

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
November 24, 2025 • 8:30 PM

