Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

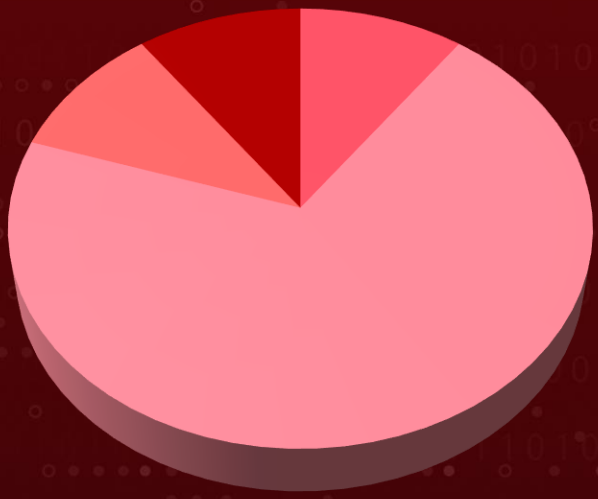
September 2026 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
September 22, 2026	A1	TA2026276

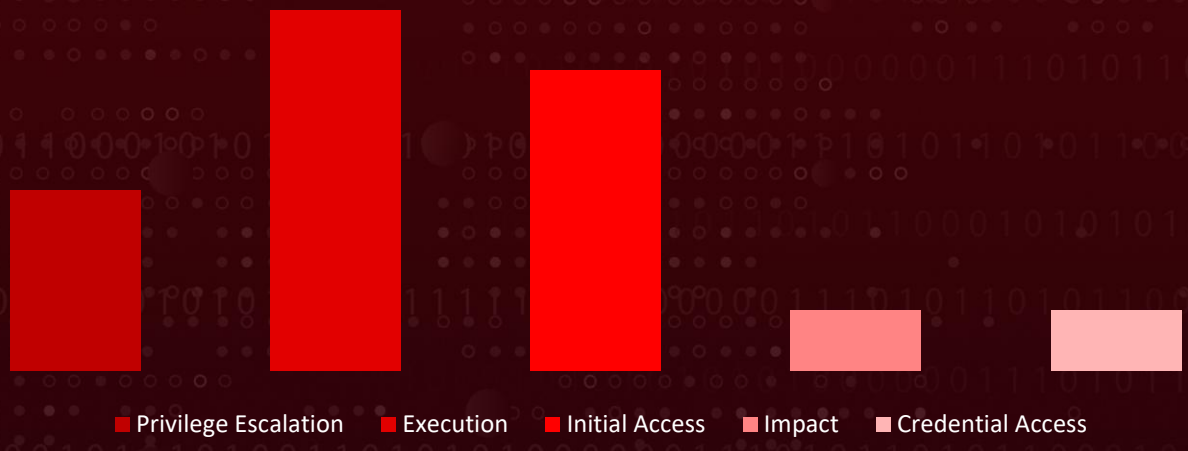
Summary

In **September**, more than **5782** 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 **352** 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-2025-8088*	RARLAB WinRAR Path Traversal Vulnerability	RARLAB WinRAR	Code Execution	Local
CVE-2026-85046*	Google Chrome V8 Type Confusion Vulnerability	Google Chrome	Code Execution	Network
CVE-2026-87491*	Google Chromium V8 Out of Bounds Write Vulnerability	Google Chrome (V8 Engine)	Code Execution	Network
CVE-2025-39964*	Linux Kernel Race Condition Vulnerability	Linux kernel	Data Interleaving and Corruption	Local
CVE-2025-62593*	Ray-Project Ray Code Injection Vulnerability	Ray-Project Ray	Code Execution	Network
CVE-2026-48710*	Kludex Starlette HTTP Request/Response Smuggling Vulnerability	Kludex Starlette	Expose Sensitive Data	Network
CVE-2026-53266*	Linux Kernel Out-of Bounds Write Vulnerability	Linux kernel	Code Execution	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-2026-53362*	Linux Kernel Unspecified Vulnerability	Linux kernel	Code Execution	Local
CVE-2026-64849*	MLflow Server-Side Request Forgery Vulnerability	MLflow	Server-Side Request Forgery	Network
CVE-2026-66897	Canonical LXD Path Traversal Vulnerability	Canonical LXD	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.

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-39964</td><td>✗</td><td rowspan="2">Linux Kernel, SUSE, Debian, Redhat, Ubuntu</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*
cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:*:*
cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:*:*
cpe:2.3:o:opensuse:leap:*:*:*:*:*:*:*:*:*
cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Linux Kernel Race Condition Vulnerability</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-362</td><td>T1499: Endpoint Denial of Service</td><td>SUSE, Debian, Redhat, Ubuntu</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-62593		Ray Prior to version 2.52.0, Redhat	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:anyscale:ray:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*	RondoDox ShadowRay 2.0
Ray-Project Ray Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94, CWE-352	T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter	RHEL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-8088		WinRAR Versions up to and including 7.12, SUSE	Amaranth-Dragon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:* cpe:2.3:o:suse:sles:*:*:*:*:*:*:*:*	Amaranth Loader, TGAmaranth RAT
RARLAB WinRAR Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-35	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	Winrar, SUSE

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-48710	BadHost	Kludex Starlette Prior to version 1.0.1, Redhat	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:encode:starlette:*:*:*:*:*:*:python:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*	-
Kludex Starlette HTTP Request/Response Smuggling Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1289, CWE-444	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	RHEL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-53266	✗	Linux Kernel Version before 5.10, Ubuntu	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-53362		Linux kernel, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:*	-
Linux Kernel Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-122, CWE-787	T1068: Exploitation for Privilege Escalation	Linux Kernel, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-64849		MLflow (Before 3.15.0), Redhat	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mlflow:mlflow:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*	-
MLflow Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	mlflow, RHEL

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-85046		Google Chrome (Before 152.0.7977.82 Linux; Before 152.0.7977.82/.83 Windows, macOS)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:*	-
Google Chrome V8 Type Confusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1190:Exploit Public-Facing Application, T1059.007 Command and Scripting Interpreter: JavaScript	Chrome

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-87491	 ZERO-DAY	Google Chrome versions before 153.0.8010.36 on Windows, macOS, and Linux	TA412, UTA0560, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	GRIMWEDGE, SUPERSTOMP, LONGTALE (aka GemStone), ShadowPad
Google Chromium V8 Out of Bounds Write Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-787	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	Chrome

Vulnerability Details

#1

September was a busy month for the Linux ecosystem, with over 5782 vulnerabilities patched across major distributions and products, ranging from information disclosure bugs to privilege escalation and remote code execution flaws. Out of these, HiveForce Labs flagged 10 critical vulnerabilities that are either already being exploited or likely to be targeted soon, with three confirmed under active attack.

#2

Chrome users face a more serious threat: two V8 zero-days, CVE-2026-85046 (a type confusion bug) and CVE-2026-87491 (an out-of-bounds write flaw), both allow remote code execution inside the sandbox via a malicious webpage. What makes CVE-2026-87491 especially dangerous is that it's used as part of a full exploit chain called BlueMoon, combining it with CVE-2026-85046 and a Windows kernel privilege escalation bug (CVE-2026-85880) to compromise a machine with a single click.

#3

BlueMoon first surfaced on August 28, 2026, used by the China-linked group TA412 (also known as JungleBamboo or APT31), and was quickly picked up by several other espionage-focused actors, UTA0560, UNK_LateNight, UNK_DoubleCheck, and UNK_QuietRacket. Payloads delivered through this chain include the GRIMWEDGE backdoor, the SUPERSTOMP loader (which installs the credential-stealing LONGTALE/GemStone Chrome extension), ShadowPad, and various Rust-based loaders. Targets span NGOs, US aerospace and defense firms, mining and commodity trading companies, Vietnamese manufacturers, and government and financial institutions in Indonesia and Singapore.

#4

CVE-2025-8088 is another zero-day flaw: a path traversal flaw in the Windows version of WinRAR that lets attackers run arbitrary code through specially crafted archive files.

#5

On the Linux kernel side, CVE-2025-39964 fixes a race condition in af_alg sockets where concurrent writes could corrupt internal state, the fix now enforces exclusive write ownership. Separately, CVE-2026-53266 is a memory corruption bug in netfilter's bridge ebtables SNAT target, and CVE-2026-53362 is a buffer overflow in the IPv6 stack that lets an unprivileged local user trigger kernel corruption via crafted UDPv6 traffic.

#6

A few application-layer flaws also stand out. CVE-2025-62593 affects Ray (the AI compute engine), its browser-based defense relies on checking the User-Agent header, which turns out to be trivially spoofable, making it exploitable via DNS rebinding against developers who visit a malicious site. It's fixed in version 2.52.0. CVE-2026-48710 in the Starlette framework stems from unvalidated Host headers, which could let attackers bypass security checks that rely on the reconstructed request URL, patched in 1.0.1.

#7

Rounding it out, CVE-2026-64849 in MLflow allows attackers to bypass webhook URL validation through redirects, potentially exposing internal or cloud metadata services. And CVE-2026-66897 is a critical path traversal bug in Canonical LXD that lets an attacker with container access overwrite host files as root, leading to full host compromise.

#8

With active exploitation confirmed on three fronts, especially the Chrome/BlueMoon chain, patching WinRAR, Chrome, and the affected Linux kernel builds should be treated as a top priority this cycle. Timely patching, strict configuration hardening, and defense-in-depth strategies remain essential to prevent system compromise.

Recommendations

Proactive Strategies:

- Patch Actively Exploited Zero-Days First: Prioritize WinRAR, Chrome (CVE-2026-85046, CVE-2026-87491), and the affected Linux kernel builds ahead of routine patch cycles, since these are already being exploited in the wild.
- Enable Auto-Updates on High-Risk Applications: Configure browsers and frequently targeted software to update automatically, shrinking the window attackers have to exploit newly disclosed zero-days.
- Validate Redirects on Webhook Endpoints: Pin and re-verify the resolved destination after redirects for services like MLflow, so SSRF techniques can't be used to reach internal or cloud metadata services.
- Restrict Container and Template Permissions: Limit who can edit or launch container images in platforms like LXD, reducing the risk of host-level compromise through path traversal flaws.
- Isolate Developer Tools from General Browsing: Keep AI/ML platforms such as Ray on separate networks or machines from everyday browsing to limit exposure to malvertising and DNS rebinding attacks.
- Deploy Detection for Multi-Stage Exploit Chains: Use EDR tooling capable of flagging chained exploitation behavior, since attacks like BlueMoon combine several CVEs to achieve full compromise from a single click.

Reactive Strategies:

- Isolate Hosts Showing Compromise Indicators: If payloads like GRIMWEDGE, SUPERSTOMP, or ShadowPad are detected, disconnect the affected endpoint immediately to stop lateral movement.
- Rotate Exposed Credentials and Sessions: After detecting credential-stealing tools like the LONGTALE/GemStone extension, reset all potentially exposed passwords, tokens, and active sessions.
- Hunt for Known Threat Actor Indicators: Proactively search logs and endpoints for IOCs tied to TA412 and related clusters to catch any compromise that evaded initial detection.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-8088*	T1204: User Execution, T1204.002: Malicious File, T1059: Command and Scripting Interpreter	DET0294 - User Execution – Malicious File via download/open → spawn chain (T1204.002), DET0516 - Behavioral Detection of Command and Scripting Interpreter Abuse	M1038 - Execution Prevention	Winrar, SUSE
CVE-2026-85046*	T1190:Exploit Public-Facing Application, T1059.007 Command and Scripting Interpreter: JavaScript	DET0080 - Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0264 - Cross-Platform Detection of JavaScript Execution Abuse	M1051 - Update Software, M1038 - Execution Prevention	Chrome

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-87491*	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, M1038 - Execution Prevention	Chrome
CVE-2025-39964*	T1499: Endpoint Denial of Service	DET0208 - Endpoint Resource Saturation and Crash Pattern Detection Across Platforms	M1037 - Filter Network Traffic	SUSE, Debian, Redhat, Ubuntu
CVE-2025-62593*	T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter	DET0176 - Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189), DET0516 - Behavioral Detection of Command and Scripting Interpreter Abuse	M1051 - Update Software, M1038 - Execution Prevention	RHEL
CVE-2026-48710*	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	DET0516 - Behavioral Detection of Command and Scripting Interpreter Abuse, DET0514 - Detection Strategy for Exploitation for Privilege Escalation	M1045 - Code Signing	RHEL

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-53266*	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	DET0516 - Behavioral Detection of Command and Scripting Interpreter Abuse, DET0514 - Detection Strategy for Exploitation for Privilege Escalation	M1045 - Code Signing	Ubuntu
CVE-2026-53362*	T1068: Exploitation for Privilege Escalation	DET0514 - Detection Strategy for Exploitation for Privilege Escalation	M1038 - Execution Prevention, M1050 - Exploit Protection	Linux Kernel, Ubuntu
CVE-2026-64849*	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	DET0080 - Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0412 - Detect Access or Search for Unsecured Credentials Across Platforms	M1030 - Network Segmentation, M1051 - Update Software, M1035 - Limit Access to Resource Over Network	mlflow, RHEL
CVE-2026-66897	T1068: Exploitation for Privilege Escalation	DET0514 - Detection Strategy for Exploitation for Privilege Escalation	M1038 - Execution Prevention, M1051 - Update Software	Debian, Ubuntu

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/

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 Demo of **HivePro**.

REPORT GENERATED ON

September 22, 2026 • 03:00 AM

More at www.hivepro.com