

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

July 2026 Linux Patch Roundup

Date of Publication

July 23, 2026

Admiralty Code

A1

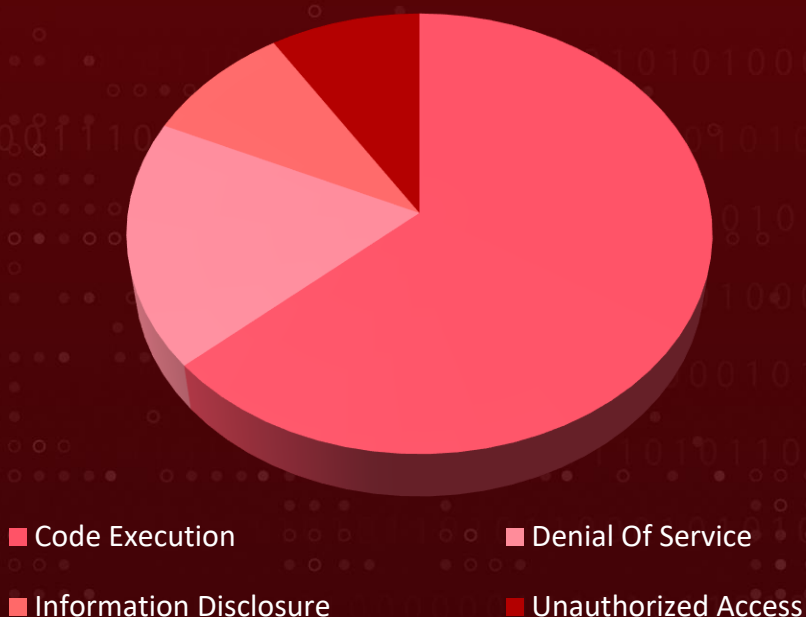
TA Number

TA2026210

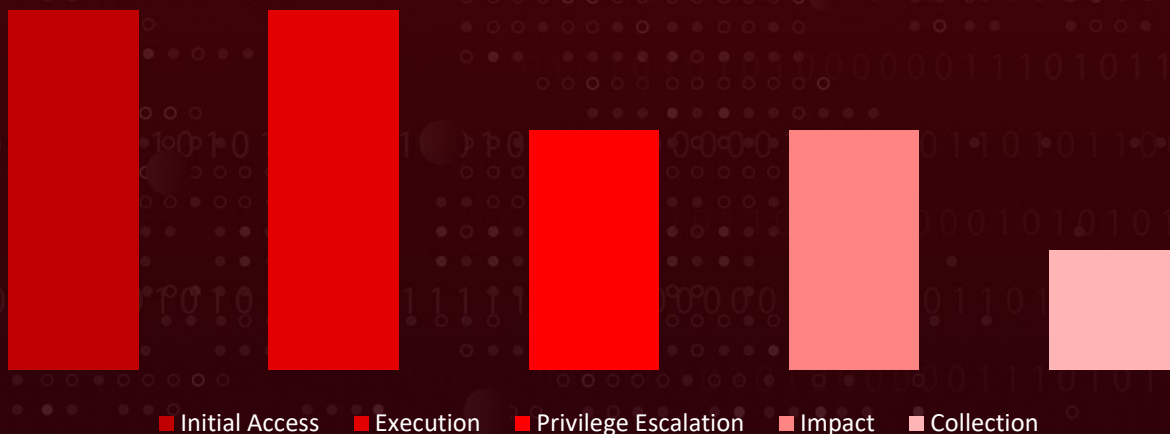
Summary

In **July**, more than **3627** 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 **433** 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 **11 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-2026-0915	GNU C Library Information Disclosure Vulnerability	Debian, RedHat, Alma Linux, Rocky Linux, Ubuntu	Information Disclosure	Network
CVE-2026-13774	Chrome Extensions Use-After-Free Vulnerability	Chrome, Debian	Code Execution	Network
CVE-2026-20213	ClamAV PE Parser DoS Vulnerability	Cisco, Ubuntu, Debian	Denial Of Service	Network
CVE-2026-34980	OpenPrinting CUPS Auth Bypass Vulnerability	OpenPrinting, Ubuntu, Rocky Linux, RedHat, Debian, Alpine Linux	Unauthorized Access	Network
CVE-2026-42271*	BerriAI LiteLLM Command Injection Vulnerability	BerriAI LiteLLM, RedHat	Code Execution	Network
CVE-2026-43499*	GhostLock (Linux Kernel rtmutex Use-After-Free Vulnerability)	Linux Kernel, Debian, Alma Linux, RedHat, Rocky Linux, Ubuntu	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-2026-4480	Samba Printing Subsystem OS Command Injection Vulnerability	Debian, Alma Linux, RedHat, Alpine Linux, Rocky Linux, Ubuntu	Code Execution	Network
<u>CVE-2026-46242*</u>	Bad Epoll (Linux Kernel Use After Free Vulnerability)	Linux kernel, Ubuntu, RedHat, Debian, Alma Linux	Code Execution	Local
CVE-2026-46529	Atril Polyglot-PDF Single-Click RCE Vulnerability	Ubuntu, Rocky Linux, RedHat, Debian, Alpine Linux	Remote Code Execution	Local
CVE-2026-5950	BIND 9 Unbounded Resend Loop DoS Vulnerability	Ubuntu, RedHat, Debian, Alpine Linux	Denial Of Service	Network
CVE-2026-55200	libssh2 Unchecked packet_length Out-of-Bounds Write Vulnerability	libssh2, Debian, Ubuntu, RedHat	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.

n the CISA

KEV catalog, used in malware operations, or targeted by threat actors in their campaigns.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-46242</u>	Bad Epoll	Linux kernel, Ubuntu, RedHat, Debian, Alma 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:redhat:enterprise_linux:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*	-
Bad Epoll (Linux Kernel Use After Free Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities, T1588.006: Vulnerabilities	Linux Kernel , Ubuntu , RedHat , Debian , Alma Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-42271		BerriAI LiteLLM, RedHat	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:litellm:litellm:*:*:*:*:*:*:*	-
BerriAI LiteLLM Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1552: Unsecured Credentials, T1552.001: Credentials In Files	BerriAI LiteLLM

Vulnerability Details

#1

In July, the Linux ecosystem addressed over **4,060** vulnerabilities across various distributions and products, covering critical issues such as information disclosure, denial-of-service, and code execution. Over **3,627** new vulnerabilities were discovered and patched. HiveForce lab has identified **11** critical vulnerabilities that are either currently being exploited or are highly likely to be exploited in the near future.

#2

These vulnerabilities could facilitate adversarial tactics such as Initial Access, Execution, and Privilege Escalation. Notably, **three** of these vulnerabilities are currently being exploited, requiring urgent attention and remediation.

#3

GhostLock (CVE-2026-43499) is a 15-year-old Linux kernel bug that lets any logged-in user seize full root control of a machine. The flawed code has shipped by default in nearly every major Linux distribution since 2011. GhostLock is also the second half of an exploit chain called IonStack. The first half, CVE-2026-10702, is a Firefox flaw that runs code inside the browser and breaks out of its sandbox; GhostLock then carries the attacker the rest of the way to root.

#4

Bad Epoll (CVE-2026-46242) is another Linux kernel flaw that lets a regular user with no special access take over a machine as root. It affects Linux desktops, servers, and Android, and a patch is available. Epoll is a core Linux feature that lets a program monitor many files or network connections at once. Servers, network services, and web browsers all depend on it, so it can't simply be turned off.

#5

CVE-2026-42271 is a command injection flaw in LiteLLM that lets any authenticated user run arbitrary commands on the host. A successful attack could let intruders execute commands on the LiteLLM server, steal model-provider credentials, harvest API keys and secrets held by the proxy, pivot into connected AI infrastructure, and compromise downstream systems linked to the gateway.

#6

CVE-2026-13774 is a use-after-free flaw in Google Chrome's Extensions component. The root cause is poor object lifetime management: a pointer to an extension-related object stays reachable after the object has been destroyed, so a later operation ends up reading or writing freed memory.

Recommendations

Proactive Strategies:



Patch Promptly: Upgrade to fixed versions across all listed products: Chrome $\geq 150.0.7871.47$, LiteLLM $\geq 1.83.7$, patched Linux kernels for GhostLock (CVE-2026-43499) and Bad Epoll (CVE-2026-46242), glibc updates via distro advisories, and the ClamAV and CUPS releases as soon as vendors publish them.



Least-Privilege Access: Restrict local shell access on Linux hosts (limits GhostLock and Bad Epoll blast radius), run LiteLLM as an unprivileged, sandboxed user, and issue proxy API keys with the minimum scope required.



Browser Extension Governance: Enforce Chrome ExtensionInstallAllowlist / ExtensionInstallBlocklist policies so only vetted extensions can be installed; disable third-party extension sideloading.



Harden Configurations: Disable the DNS backend for the networks NSS database in nsswitch.conf unless required; require authentication for all CUPS print submissions; disable ClamAV PE scanning temporarily where operationally acceptable if a patch is delayed.

Reactive Strategies:



Centralized Logging and SIEM Correlation: Forward kernel ring buffer, CUPS access logs, ClamAV daemon logs, LiteLLM audit logs, DNS query logs, and endpoint process telemetry to a SIEM. Correlate crashes and anomalies to vulnerable versions.



Credential Rotation on Suspicion: If a LiteLLM host is suspected of compromise, immediately rotate proxy API keys, model-provider credentials, and any secrets reachable by the process; audit /mcp-rest/test/* request bodies for command, args, or env fields.



Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-0915	T1005: Data from Local System	<u>DET0380: Detection of Local Data Collection Prior to Exfiltration</u>	<u>M1057: Data Loss Prevention</u>	 <u>Debian, RedHat, Alma Linux, Rocky Linux, Ubuntu</u>
CVE-2026-13774	T1203: Exploitation for Client Execution	<u>DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)</u>	<u>M1048: Application Isolation and Sandboxing, M1050: Exploit Protection</u>	 <u>Chrome, Debian</u>
CVE-2026-20213	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	<u>DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms, DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation</u>	<u>M1037: Filter Network Traffic</u>	 <u>Cisco, Ubuntu, Debian</u>
CVE-2026-34980	T1190: Exploit Public-Facing Application	<u>DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)</u>	<u>M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic</u>	 <u>OpenPrinting, Ubuntu, Rocky Linux, RedHat, Debian, Alpine Linux</u>



CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-42271*	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1552: Unsecured Credentials, T1552.001: Credentials In Files	<u>DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)</u>	<u>M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic</u>	 BerriAI LiteLLM  RedHat
CVE-2026-43499*	T1068: Exploitation for Privilege Escalation	<u>DET0514: Detection Strategy for Exploitation for Privilege Escalation</u>	<u>M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection</u>	 Linux Kernel, Debian, Alma Linux, RedHat, Rocky Linux, Ubuntu
CVE-2026-4480	T1190: Exploit Public-Facing Application	<u>DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)</u>	<u>M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic</u>	 Debian, Alma Linux, RedHat, Alpine Linux, Rocky Linux, Ubuntu

CVE ID	TTPs	Detection	Mitigation	Patch
<u>CVE-2026-46242*</u>	T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities, T1588.006: Vulnerabilities	<u>DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0850: Detection of Obtain Capabilities</u>	<u>M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection, M1056: Pre-compromise</u>	 <u>Linux Kernel, Ubuntu, RedHat, Debian, Alma Linux</u>
CVE-2026-46529	T1203: Exploitation for Client Execution	<u>DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)</u>	<u>M1048: Application Isolation and Sandboxing, M1050: Exploit Protection</u>	 <u>Ubuntu, Rocky Linux, RedHat, Debian, Alpine Linux</u>
CVE-2026-5950	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	<u>DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms</u>	<u>M1037: Filter Network Traffic</u>	 <u>Ubuntu, RedHat, Debian, Alpine Linux</u>
CVE-2026-55200	T1203: Exploitation for Client Execution	<u>DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)</u>	<u>M1048: Application Isolation and Sandboxing, M1050: Exploit Protection</u>	 <u>libssh2, Debian, Ubuntu, RedHat</u>

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://nebusec.ai/research/ionstack-part-2/>

<https://www.hivepro.com/threat-advisory/bad-epoll-linux-kernel-eventpoll-use-after-free-enables-local-root>

<https://github.com/NebuSec/CyberMeowfia/tree/main/IonStack/CVE-2026-43499>

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

July 23, 2026 • 7:00 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com