Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

August 2026 Linux Patch Roundup

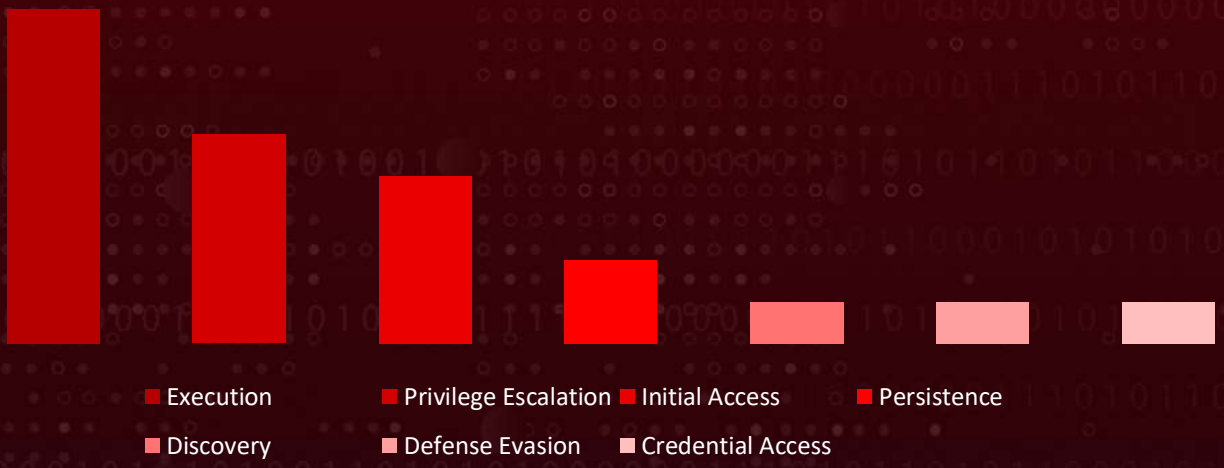
Date of Publication	Admiralty Code	TA Number
August 25, 2026	A1	TA2026243

Summary

In **August**, more than **3221** 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 **3361** 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 9 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-2026-31431*	Copy Fail (Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability)	Linux, Debian, RedHat, SUSE, Ubuntu	Privilege Escalation	Local
CVE-2026-43494	PinTheft (Linux Kernel RDS Double-Free Vulnerability)	Linux, Ubuntu, SUSE, RedHat, Debian	Privilege Escalation	Local
CVE-2026-4631	Cockpit SSH Argument Injection Remote Code Execution Vulnerability	Cockpit, RedHat, SUSE, Debian	Code Execution	Network
CVE-2026-60137*	wp2shell (WordPress Core SQL Injection Vulnerability)	WordPress, Debian, Ubuntu	Code Execution	Network
CVE-2026-64531	OVSwrap (Linux Kernel Open vSwitch Denial-of-Service Vulnerability)	Linux, RedHat, Debian, Ubuntu	Denial-of-Service	Local
CVE-2026-64564	SCTPhantom (Linux Kernel SCTP Use-After-Free Vulnerability)	Linux, RedHat, Debian, Ubuntu	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-2026-64600	RefluXFS (Linux Kernel XFS Race Condition Vulnerability)	Linux, RedHat, Oracle Amazon	Privilege Escalation	Local
CVE-2026-66066	KindaRails2Shell (Ruby on Rails Active Storage Remote Code Execution Vulnerability)	Ruby on Rails, Debian, Ubuntu	Code Execution	Network
CVE-2026-77647*	SPIP Code Injection Vulnerability	SPIP, Debian, Ubuntu	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-2026-31431	Copy Fail	Linux Kernel versions shipped from 2017 through 6.18.21 and 6.19.11; fixed in 6.18.22, 6.19.12, and 7.0), Debian, RedHat, SUSE, Ubuntu	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*	-
Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-669, CWE-1288	T1068: Exploitation for Privilege Escalation, T1611: Escape to Host, T1059.004: Unix Shell	Linux Kernel, Debian, RedHat, SUSE, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-60137	wp2shell	WordPress WordPress Core (Version before 6.9.5 and 7.0.2), Debian, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:*	-
WordPress Core SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-89	T1190: Exploit Public-Facing Application, T1136.001: Create Account: Local Account, T1059: Command and Scripting Interpreter	WordPress, Debian, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-77647		SPIP before 4.4.20, Debian, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:spip:spip:*:*:*:*:*:*:*:* cpe:2.3:o:ubuntu_linux:*:*:*:*:*:*:*:*cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:*	-
SPIP Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003: Web Shell	SPIP, Debian, Ubuntu

Vulnerability Details

#1

In August, the Linux ecosystem addressed over 3361 vulnerabilities across major distributions and products, spanning issues from information disclosure to privilege escalation to remote code execution. HiveForce Labs has identified 9 critical vulnerabilities that are either currently being exploited or highly likely to be targeted soon. Notably, three of these are under active exploitation, requiring immediate attention and remediation.

#2

The most urgent threats are unauthenticated, network-reachable code-execution flaws already being abused in the wild. CVE-2026-77647, a critical code-injection vulnerability (CVSS 9.8, CWE-94) in the SPIP content management system, allows a remote, unauthenticated attacker to execute arbitrary code on the server through a crafted request and is confirmed exploited in the wild as of August 2026; it is fixed in SPIP 4.4.20 and is the clearest emergency-remediation case in this set.

#3

Alongside it, CVE-2026-60137, tracked as "wp2shell", is a critical SQL injection flaw (CVSS 9.1) in WordPress core's WP_Query author__not_in handling that chains to full remote code execution by forging a malicious administrator account; exploitation has been observed since mid-July, affects the single largest web-application footprint on the internet, and is resolved in WordPress 6.9.5, 7.0.2, and 6.8.6.

#4

Other network-facing services present the next tier of remote-code-execution risk even where in-the-wild abuse has not yet been confirmed. CVE-2026-4631, an unauthenticated argument-injection flaw in Cockpit (CVSS 9.8), lets a remote attacker smuggle attacker-controlled options into an SSH invocation and achieve command execution against Cockpit 327 and later fronted by OpenSSH earlier than 9.6; it is fixed in Cockpit 360.

#5

CVE-2026-66066, "KindaRails2Shell", is a critical Ruby on Rails Active Storage flaw (CVSS 9.5) in which an attacker-supplied image drives libvips to read arbitrary files, recovering the application's signing secrets and pivoting to unauthenticated remote code execution; a public proof-of-concept and a Metasploit module already exist, and Debian, Ubuntu, and default Rails container images are exposed out of the box. It is fixed in Rails 7.2.3.2, 8.0.5.1, and 8.1.3.1 with libvips 8.13 or later, and all secrets the application can read should be rotated.

#6

The Linux kernel remains the primary target for local privilege escalation, and this month's set is unusually deep. CVE-2026-31431, "Copy Fail," is a memory-corruption flaw in the kernel's algif_aead (AF_ALG) crypto interface that grants root from an unprivileged local context; it is already under active exploitation and carries added weight in containerized environments.

#7

CVE-2026-64600, "RefluXFS," is a race condition in the XFS reflink copy-on-write path that overwrites a protected file such as /etc/passwd or a SUID-root binary directly in the block layer to obtain root; it is especially dangerous because exploitation produces no kernel log output and is not blocked by SELinux in enforcing mode, and because XFS reflink is the default on Red Hat Enterprise Linux and its derivatives. CVE-2026-64564, "SCTPhantom," is an 18-year-old use-after-free in the kernel's SCTP ASCONF handling that yields both local privilege escalation and container escape.

#8

CVE-2026-64531, "OVSwrap," abuses unprivileged user namespaces to auto-load the Open vSwitch kernel module and corrupt nested-attribute handling, causing kernel memory corruption and denial of service, and CVE-2026-43494, "PinTheft," chains a double-free in the kernel's RDS sockets with io_uring to overwrite a privileged binary's page cache and escalate to root. The latter four, RefluXFS, SCTPhantom, OVSwrap, and PinTheft, carry public proof-of-concept code but are not yet confirmed exploited in the wild.

#9

August 2026's vulnerability landscape reflects continued high-risk trends, with active exploitation of internet-facing web applications, weaponized kernel privilege-escalation flaws, and unauthenticated remote code execution in network services and application dependencies posing the most urgent threats. Timely patching, strict configuration hardening, and defense-in-depth strategies remain essential to prevent system compromise.

Recommendations

Proactive Strategies:

Patch Actively Exploited Flaws First: SPIP (CVE-2026-77647), WordPress "wp2shell" (CVE-2026-60137), and "Copy Fail" (CVE-2026-31431) are under active exploitation. Upgrade to SPIP 4.4.20 and WordPress 6.9.5/7.0.2/6.8.6, and apply the kernel update for Copy Fail. Treat exposed vulnerable systems as emergencies.

Rotate Secrets After Framework Exposure: KindaRails2Shell reaches remote code execution by reading the application's signing material off disk, so patching alone does not close the risk. Rotate secret_key_base, database credentials, API keys, and any other secret the application process can read on hosts that ran a vulnerable Rails build. Assume disclosed secrets are compromised.

Harden and Update the Kernel Against Local Privilege Escalation: Five kernel flaws (Copy Fail, RefluXFS, SCTPhantom, PinTheft) grant local root, some with container escape. Apply kernel updates, and where you can't, reduce surface: restrict unprivileged user namespaces (OVSwrap) and blacklist unused sctp and rds modules (SCTPhantom, PinTheft).

Prioritize Patching Where Detection Will Fail: RefluXFS (CVE-2026-64600) overwrites protected files directly in the block layer, producing no kernel log output and running past SELinux in enforcing mode, it cannot be reliably caught at runtime and there is no configuration toggle to mitigate it. On Red Hat Enterprise Linux and its derivatives, where XFS reflink is the default, apply the kernel fix as the only dependable control and back it with file-integrity monitoring of /etc/passwd and SUID-root binaries.

Reactive Strategies:

System Isolation and Containment: Immediately isolate affected workloads, containers, or management servers to prevent further spread. In cloud environments, quarantine compromised nodes and restrict API interactions until integrity is restored.

Deploy Network Traffic Analysis for Unusual Patterns: Continuously monitor inbound and outbound network traffic to detect anomalies such as unexpected SSH connections, unusual data flows, or communication over non-standard ports. Establish behavioral baselines for normal traffic and configure alerts for deviations, as these may indicate exploitation attempts targeting vulnerabilities. Integrating NTA with SIEM/EDR platforms enhances real-time detection and rapid response.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-31431*	T1068: Exploitation for Privilege Escalation, T1611: Escape to Host, T1059.004: Unix Shell	DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software, M1048: Application Isolation and Sandboxing, M1038: Execution Prevention	Linux, Debian, RedHat, SUSE, Ubuntu, Amazon
CVE-2026-43494	T1068: Exploitation for Privilege Escalation, T1059.004: Unix Shell	DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software, M1042: Disable or Remove Feature or Program, M1048: Application Isolation and Sandboxing	Linux, Ubuntu, SUSE, RedHat, Debian
CVE-2026-4631	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	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, M1030: Network Segmentation, M1054: Software Configuration	Cockpit, RedHat, SUSE, Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-60137*	T1190: Exploit Public-Facing Application, T1136.001: Create Account: Local Account, 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, M1030: Network Segmentation, M1016: Vulnerability Scanning	WordPress, Debian, Ubuntu
CVE-2026-64531	T1499: Endpoint Denial of Service, T1068: Exploitation for Privilege Escalation	DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms, DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software M1017: User Training M1021: Restrict Web-Based Content	RedHat, Debian, Ubuntu, SUSE
CVE-2026-64564	T1068: Exploitation for Privilege Escalation, T1611: Escape to Host, T1059.004: Unix Shell	DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software, M1042: Disable or Remove Feature or Program, M1048: Application Isolation and Sandboxing	RedHat, Debian, Ubuntu, SUSE, Amazon

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-64600	T1068: Exploitation for Privilege Escalation, T1548.001: Setuid and Setgid, T1222.002: Linux and Mac File and Directory Permissions Modification	DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software, M1038: Execution Prevention	Linux, RedHat, Oracle, Amazon
CVE-2026-66066	T1190: Exploit Public-Facing Application, T1083: File and Directory Discovery, T1552.001: Credentials In Files, 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, M1022: Restrict File and Directory Permissions, M1016: Vulnerability Scanning	Ruby on Rails, Debian, Ubuntu
CVE-2026-77647	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1505.003: Web Shell	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0027: Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets	M1051: Update Software, M1030: Network Segmentation, M1050: Exploit Protection, M1049: Antivirus/Antimalware	SPIP, 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/

https://hivepro.com/threat-advisory/one-script-every-distro-full-root-copy-fail-vulnerability-rewriting-linux-threat-models/

http://www.hivepro.com/threat-advisory/wp2shell-one-request-no-login-full-control-of-wordpress-core

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

August 25, 2026 • 03:00 AM

More at www.hivepro.com