Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

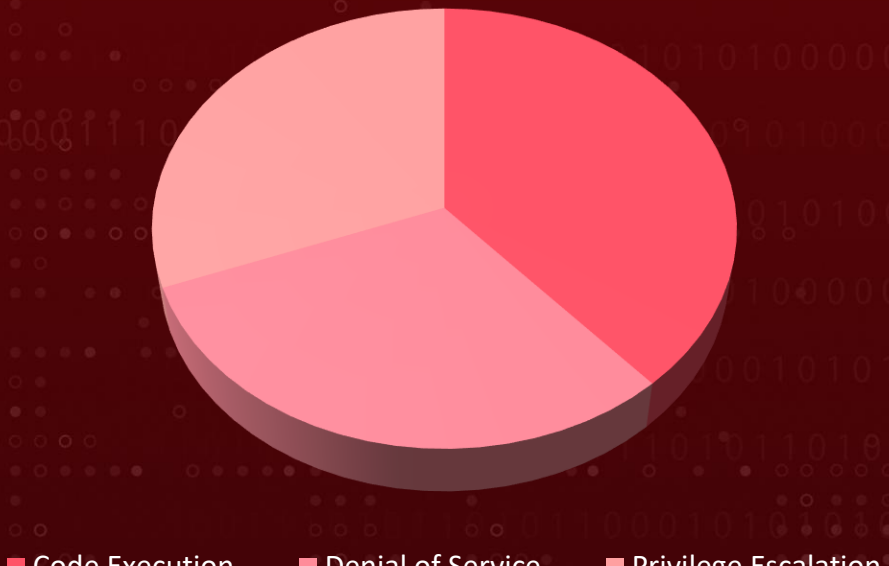
October 2026 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
October 30, 2026	A1	TA2026321

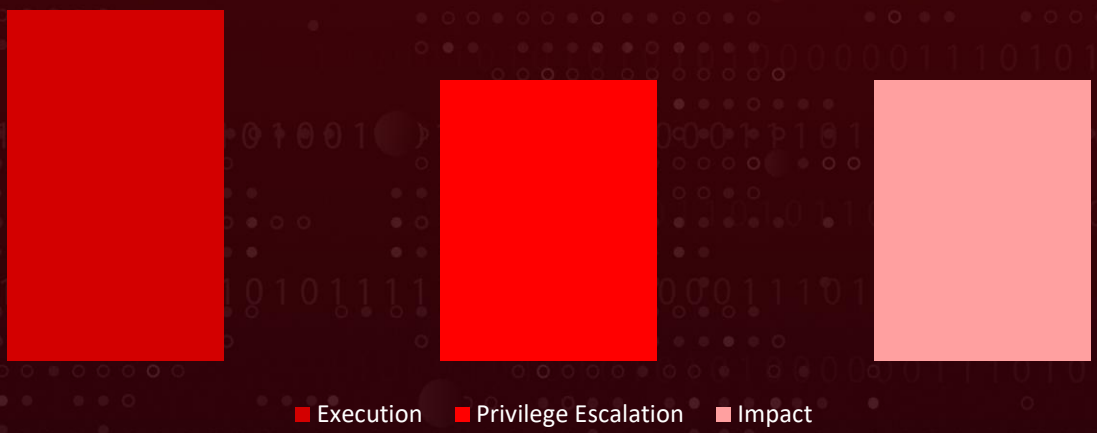
Summary

In **October**, more than **8369** 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 **432** 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 for 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-2026-0908	Chromium Use after free in ANGLE Vulnerability	Alma Linux, Alpine Linux, Debian, Redhat, Rockylinux	Code Execution	Network
CVE-2026-23479	Redis use-after-free (UAF) vulnerability	Redhat, Rocky Linux, Ubuntu, Debian, Alpine Linux, Alma Linux	Code Execution	Network
CVE-2026-17653	Chromium use-after-free Vulnerability	Rocky Linux, Redhat, Debian, Alma Linux	Code Execution	Network
CVE-2026-17655	Chromium Insufficient Input Validation Vulnerability	Rocky Linux, Redhat, Debian, Alma Linux	Code Execution	Network
CVE-2026-25243	Redis Heap-Based Buffer Overflow Vulnerability	Redis, Ubuntu, Rocky Linux, Redhat, Debian, Alpine Linux	Code Execution	Network
CVE-2026-46242	Linux Kernel Eventpoll Subsystem Use-After-Free Vulnerability	Ubuntu, Redhat, Debian, Alma Linux, Linux Kernel	Privilege Escalation	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-2026-64564*	SCTPhantom (Linux kernel SCTP Use-After-Free Vulnerability)	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	Privilege Escalation	Network
CVE-2026-74480	Linux Kernel Bridge Multicast Subsystem Use-After-Free Vulnerability	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	Denial of Service	Network
CVE-2026-74581	Linux Kernel IPv6 Routing Subsystem Use-After-Free Vulnerability	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	Denial of Service	Network
CVE-2026-80714	Linux Kernel IPVS Subsystem Use-After-Free Vulnerability	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	Denial of Service	Network
CVE-2026-81642	NLnet Labs Unbound Heap-Based Buffer Overflow Vulnerability	NLnet Labs, Ubuntu, Redhat, Rocky Linux, Debian, Alpine Linux, Alma Linux	Denial of Service	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-2026-87902*	WordPress Core Remote File Inclusion Vulnerability	WordPress, Debian, Ubuntu	Privilege Escalation	Network
CVE-2026-64561*	Zapscape (Linux Kernel KVM Subsystem Privilege Escalation Vulnerability)	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	Privilege Escalation	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.

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-2026-87902*		WordPress Core (4.7.0 -7.1.1), Debian, Ubuntu	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:*:* cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*:*	-
WordPress Core Remote File Inclusion Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-98	T1190: Exploit Public-Facing Application, T1505.003: Web Shell	WordPress, Debian, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-64564*	SCTPhantom ZERO-DAY	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:resf:rocky_linux:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:* cpe:2.3:o:almalinux:almalinux:*:*:*:*:*:*:*:*	-
SCTPhantom (Linux kernel SCTP Use-After-Free Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1068: Exploitation for Privilege Escalation, T1611: Escape to Host	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-64561*	Zapscape	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	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:resf:rocky_linux:*:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*:* cpe:2.3:o:almalinux:almalinux:*:*:*:*:*:*:*:*:*	-
Zapscape (Linux Kernel KVM Subsystem Privilege Escalation Vulnerability)	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-362	T1611: Escape to Host, T1068: Exploitation for Privilege Escalation, T1499.004: Application or System Exploitation	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux

Vulnerability Details

#1

October was a busy month for the Linux ecosystem, with over 8901 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 13 critical vulnerabilities that are either already being exploited or likely to be targeted soon, with three confirmed to be under active attack.

#2

CVE-2026-87902 is the most urgent flaw in this advisory and the only one confirmed to be exploited in the wild. It is an unauthenticated path traversal (CWE-22, CWE-98) in the WordPress Core function get_page_template(). It lets an attacker load PHP files from outside the theme directories, which can lead to remote code execution. All WordPress versions from 4.7.0 through 7.1.1 are affected. A public proof-of-concept is available, and attackers began probing sites within hours of the September 22, 2026 patch.

#3

SCTPhantom (CVE-2026-64564) is a use-after-free (CWE-416) in the Linux kernel's SCTP code that has existed since version 2.6.25. When the kernel processes an address-removal request, it validates one address but deletes the connection path chosen by another. This lets an attacker remove a path the kernel is still using, leaving a pointer to freed memory. This turned into a reliable exploit that bypasses kernel memory protections and grants root without shellcode. The same technique also lets an attacker escape a container to the host, and no special privileges or configuration changes are needed. It affects kernels before 6.6.148, 6.12.101, 6.18.42, 7.1.6, and 7.2-rc5, and was confirmed on Ubuntu, Debian, RHEL, Rocky Linux, and others. Proof-of-concept code is referenced publicly, but no attacks have been confirmed.

#4

Zapscape (CVE-2026-64561) is an expired pointer dereference (CWE-825) in the Linux kernel's KVM virtualization code. A low-privileged user inside a virtual machine can corrupt the host's memory-management data. They can then break out to the host with higher privileges or crash the hypervisor. This makes the flaw a serious risk for cloud and shared virtualization environments. It affects Linux 5.9 and later, before versions 6.6.148, 6.12.101, 6.18.42, and 7.1.6.

#5

The other ten vulnerabilities have patches available and no confirmed exploitation. Four are local use-after-free flaws in the Linux kernel: CVE-2026-74480 in bridge multicast, CVE-2026-74581 in IPv6 routing, CVE-2026-80714 in IPVS, and CVE-2026-46242 in eventpoll. Google Chrome has three graphics flaws, CVE-2026-0908, CVE-2026-17653, and CVE-2026-17655. They can be triggered by a malicious web page, and the last two can enable a sandbox escape. Redis has two flaws that can lead to remote code execution by an authenticated attacker, CVE-2026-23479 and CVE-2026-25243. NLnet Labs Unbound has CVE-2026-81642, which a crafted DNS record can trigger.

Recommendations

Proactive Strategies:



Patch WordPress Immediately: Upgrade every WordPress site to 7.1.2, or to the patched release for the branch you run. CVE-2026-87902 is being actively exploited and is listed in CISA KEV, so internet-facing sites come first. After patching, check web server logs for path traversal or template inclusion attempts made since September 22, 2026.



Prioritize Hypervisors and Container Hosts: Patch KVM hosts, Kubernetes nodes, and shared container platforms before other systems. Zapscape lets a guest break out to the host, and SCTPhantom lets a container break out to host root. Treat any host running untrusted workloads as exposed until it is running the fixed kernel.



Update Chrome and Edge: Make sure Google Chrome is on version 151.0.7922.72 for Windows and Mac, or 151.0.7922.71 for Linux, or later. This also covers the earlier CVE-2026-0908 fix. Apply the matching Microsoft Edge updates, enforce automatic updates through policy, and make sure users restart their browsers, so the update takes effect.



Upgrade and Lock Down Redis: Update Redis to 8.6.3, or to a distribution package that includes the fix. Both Redis flaws need an authenticated session, so rotate credentials, enforce strict ACLs, restrict the RESTORE command, and never expose Redis directly to the internet.

Reactive Strategies:



Contain Exposed WordPress Sites: Put any WordPress site that ran a vulnerable version after September 22, 2026, into maintenance mode or behind a web application firewall rule that blocks path traversal requests. Check the site for unfamiliar PHP files, unexpected template changes, new admin accounts, and web shells. Restore from a known-good backup if you find tampering.



Monitor Hosts for Privilege Escalation and Escape Activity: Use EDR and kernel audit logging to alert on unexpected changes to root privileges, processes leaving their container namespaces, usermode helper processes launched from containers, and unexplained kernel crashes or hypervisor restarts. Any of these could point to exploitation of SCTPhantom, Zapscape or the other kernel use-after-free flaws.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-0908	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution	DET0176: Drive-by Compromise — Behavior-based Multi-platform Detection Strategy (T1189), DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1021: Restrict Web-Based Content, M1051: Update Software, M1017: User Training	Alma Linux, Alpine Linux, Debian, Redhat, Rockylinux
CVE-2026-23479	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1499.004: Application or System Exploitation	DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1026: Privileged Account Management, M1051: Update Software, M1016: Vulnerability Scanning, M1042: Disable or Remove Feature or Program, M1019: Threat Intelligence Program	Redhat, Rocky Linux, Ubuntu, Debian, Alpine Linux, Alma Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-17653	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	DET0176: Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189), DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1021: Restrict Web-Based Content, M1051: Update Software, M1017: User Training, M1038: Execution Prevention, M1019: Threat Intelligence Program	Rocky Linux, Redhat, Debian, Alma Linux
CVE-2026-17655	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation	DET0176: Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189), DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps), DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1021: Restrict Web-Based Content, M1051: Update Software, M1017: User Training, M1038: Execution Prevention, M1019: Threat Intelligence Program	Rocky Linux, Redhat, Debian, Alma Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-25243	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1499.004: Application or System Exploitation	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0118: Exploitation of Remote Services – multi-platform lateral movement detection, DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1026: Privileged Account Management, M1051: Update Software, M1016: Vulnerability Scanning, M1042: Disable or Remove Feature or Program, M1019: Threat Intelligence Program	Redis, Ubuntu, Rocky Linux, Redhat, Debian, Alpine Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-46242	T1068: Exploitation for Privilege Escalation, T1611: Escape to Host	DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0219: Detection Strategy for Escape to Host	M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection, M1019: Threat Intelligence Program, M1051: Update Software, M1042: Disable or Remove Feature or Program, M1026: Privileged Account Management	Ubuntu, Redhat, Debian, Alma Linux, Linux Kernel

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-64564*	T1068: Exploitation for Privilege Escalation, T1611: Escape to Host	DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0219: Detection Strategy for Escape to Host	M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection, M1019: Threat Intelligence Program, M1051: Update Software, M1042: Disable or Remove Feature or Program, M1026: Privileged Account Management	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux
CVE-2026-74480	T1068: Exploitation for Privilege Escalation, T1499.004: Application or System Exploitation	DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation	M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection, M1019: Threat Intelligence Program, M1051: Update Software, M1037: Filter Network Traffic	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-74581	T1499.004: Application or System Exploitation, T1068: Exploitation for Privilege Escalation	DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation, DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1037: Filter Network Traffic, M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection, M1019: Threat Intelligence Program, M1051: Update Software	Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux, Linux Kernel
CVE-2026-80714	T1499.004: Application or System Exploitation, T1068: Exploitation for Privilege Escalation	DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation, DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1037: Filter Network Traffic, M1048: Application Isolation and Sandboxing, M1038: Execution Prevention, M1050: Exploit Protection, M1019: Threat Intelligence Program, M1051: Update Software	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-81642	T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1499.004: Application or System Exploitation	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0118: Exploitation of Remote Services – multi-platform lateral movement detection, DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1026: Privileged Account Management, M1051: Update Software, M1016: Vulnerability Scanning, M1042: Disable or Remove Feature or Program, M1019: Threat Intelligence Program	NLnet Labs, Ubuntu, Redhat, Rocky Linux, Debian, Alpine Linux, Alma Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-87902*	T1190: Exploit Public-Facing Application, T1505.003: Web Shell	DET0219: Detection Strategy for Escape to Host, DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0304: Detection Strategy for Endpoint DoS via Application or System Exploitation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1037: Filter Network Traffic, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1026: Privileged Account Management, M1051: Update Software, M1016: Vulnerability Scanning, M1042: Disable or Remove Feature or Program, M1018: User Account Management	WordPress, Debian, Ubuntu

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-64561*	T1611: Escape to Host, T1068: Exploitation for Privilege Escalation, T1499.004: Application or System Exploitation	DET0514: Detection Strategy for Exploitation for Privilege Escalation, DET0219: Detection Strategy for Escape to Host	M1048: Application Isolation and Sandboxing, M1042: Disable or Remove Feature or Program, M1038: Execution Prevention, M1026: Privileged Account Management, M1051: Update Software, M1050: Exploit Protection, M1019: Threat Intelligence Program, M1037: Filter Network Traffic	Linux Kernel, Ubuntu, Rocky Linux, Redhat, Debian, Alma Linux

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://www.hivepro.com/threat-advisory/race-against-the-patch-critical-wordpress-rce-exploited-within-hours

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

October 30, 2026 • 9:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com