Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Acronis Backup Plugin Flaw Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
September 17, 2026	A1	TA2026271

Summary

First Seen: September 15, 2026
Affected Products: Acronis Backup plugin for cPanel & WHM (Linux); Acronis Backup extension for Plesk (Linux)
Impact: Acronis has disclosed CVE-2026-87886, a high-severity flaw in its Backup plugin for cPanel & WHM and its Backup extension for Plesk on Linux, and confirmed that attackers are already using it. The weakness comes down to insecure file permissions, which lets a local attacker who already holds a low-privileged, authenticated foothold raise their access level on the server without any user interaction. Because cPanel, WHM, and Plesk sit at the heart of how hosting providers and managed service providers run their users' websites, databases, and mailboxes, a successful escalation on one of these servers can hand an attacker deep control over a shared hosting environment. What is clear is that exploitation has been seen in the wild in limited, targeted attacks aimed at cPanel & WHM deployments, based on a report from a potentially affected user, while the Plesk extension has shown no signs of being attacked. Fixes are available, and given the confirmed exploitation, updating without delay is the safest course.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-87886	Acronis Backup Incorrect Default Permissions Vulnerability	Acronis Backup plugin for cPanel & WHM / Acronis Backup extension for Plesk	✗	✓	✓

Vulnerability Details

#1 CVE-2026-87886 is a local privilege escalation vulnerability rooted in insecure file permissions, a weakness class tracked as CWE-276 (Incorrect Default Permissions). In practice, this means files or resources used by the Acronis backup software are set with permissions more open than they should be, giving a lower-privileged user a path to gain rights they were never meant to have.

#2 Acronis has deliberately kept the deeper technical details private for now, choosing to give administrators room to patch before more information becomes public. What the vendor and reporting do confirm is that the flaw affects the Linux versions of the software and that exploitation takes place entirely on the local system rather than remotely across the network.

#3 To abuse the flaw, an attacker needs to already be on the server with a low-privileged, authenticated account. From there, the attack requires no interaction from any other user and is considered low in complexity, meaning it does not depend on special timing or unusual conditions to succeed. Once the escalation works, the attacker can perform unauthorized actions and potentially run code with higher privileges, undermining the confidentiality and integrity of the affected system.

#4 The vulnerability carries a CVSS score of 7.8, placing it firmly in the high-severity range, and it affects the Acronis Backup plugin for cPanel & WHM in builds before 1.9.3.1021 and the Acronis Backup extension for Plesk in builds before 1.8.11.638. Acronis has stated that exploitation has been detected in the wild in limited, targeted attacks against cPanel & WHM deployments, based on a single report from a potentially affected user, with no signs so far of attacks against Plesk. Because the fix is already available and the flaw is being used by real attackers, patching should be treated as time-sensitive.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-87886	Acronis Backup plugin for cPanel & WHM (Before 1.9.3.1021); Acronis Backup extension for Plesk (Before 1.8.11.638)	cpe:2.3:a:acronis:backup_plugin_for_cpanel_and_whm:*:*:*:*:*:*:*:*, cpe:2.3:a:acronis:backup_extension_for_plesk:*:*:*:*:*:*:*:*	CWE-276

Recommendations

Update the Backup Integrations Immediately: Install the fixed builds without delay. For cPanel & WHM, upgrade the Acronis Backup plugin to version 1.9.3 HF3, and for Plesk, upgrade the Acronis Backup extension to version 1.8.11. Applying the vendor patches is the single most effective step and directly closes the vulnerability.

Prioritize cPanel & WHM Servers: Active exploitation has been confirmed against cPanel & WHM deployments specifically, so patch those systems first. Plesk deployments should still be updated promptly, but the confirmed in-the-wild activity makes cPanel & WHM the higher-priority target for immediate attention.

Review Local Accounts and Access: Because the flaw is abused from an existing low-privileged, authenticated account, audit the local and hosting accounts on affected servers. Remove unnecessary or dormant accounts, tighten access to only what each user needs, and reset credentials where there is any doubt about their integrity.

Monitor for Signs of Privilege Escalation: Acronis has not published specific indicators of compromise, so rely on behavioral monitoring rather than static IoCs. Watch server and system logs for unexpected privilege changes, unusual process execution under elevated accounts, and unexplained modifications to backup files or configurations on affected hosts.

Vulnerability Management: Maintain an accurate inventory of software versions and security patches, including third-party plugins and extensions that run on control-panel servers. Establish a routine cadence for assessing and applying updates, and evaluate the security posture of third-party vendors whose components run with elevated access, since these often sit outside standard patch cycles.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Links

https://security-advisory.acronis.com/updates/UPD-2609-3d72-20a7

https://security-advisory.acronis.com/updates/UPD-2609-efb0-50b2

https://security-advisory.acronis.com/advisories/SEC-10986

References

https://security-advisory.acronis.com/updates/UPD-2609-3d72-20a7

https://security-advisory.acronis.com/advisories/SEC-10986

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 17, 2026 • 08:15 AM

More at www.hivepro.com