AVIS DE SECURITE

Objet	Vulnérabilité importante d'élévation de privilèges dans les extensions de sauvegarde Acronis pour cPanel/WHM et Plesk, activement exploitée
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-213
TLP	WHITE

Résumé

Acronis a publié un correctif pour CVE-2026-87886, une vulnérabilité d'élévation de privilèges locale sous Linux (CVSS 7.8) affectant ses extensions de sauvegarde pour cPanel/WHM et Plesk, causée par des permissions de fichiers non sécurisées. Un attaquant authentifié à faible privilège peut exploiter cette faille sans interaction utilisateur pour obtenir des privilèges élevés. Acronis et des chercheurs tiers confirment une exploitation active limitée et ciblée contre le plugin cPanel ; aucune exploitation n'a été observée à ce jour contre l'extension Plesk. La CISA a ajouté cette vulnérabilité à son catalogue KEV le 16 septembre 2026.

Risque de sécurité

- Élévation de privilèges locale (CVE-2026-87886, CVSS 7.8, permissions de fichiers non sécurisées)
- Compromission du système hôte cPanel/WHM ou Plesk

Systèmes affectés

- Backup plugin pour cPanel & WHM (Linux) — versions antérieures au build 1.9.3.1021
- Backup extension pour Plesk — versions antérieures au build 1.8.11.638

Recommandations

Se référer au bulletin de sécurité de l'éditeur :

- https://www.helpnetsecurity.com/2026/09/16/acronis-backup-plugin-vulnerability-exploited-cve-2026-87886/
- https://www.securityweek.com/acronis-patches-exploited-vulnerability-in-cpanel-backup-plugin/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog