Autorité Nationale de Cybersécurité

Djibouti le, 03-05-2026

BULLETIN ALERTES

Object	Vulnérabilité critique dans cPanel & WHM
Réference	1464
Date de Publication	2026-05-03
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire (à distance)
- Élévation de privilèges
- Contournement de la politique de sécurité
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données

SYSTÉME AFFECTÉ :

- cPanel & WHM toutes versions supérieures à 11.40 jusqu'à 11.86.0.40 inclus
- cPanel & WHM versions 11.110.0 jusqu'à 11.110.0.96 inclus
- cPanel & WHM versions 11.118.0 jusqu'à 11.118.0.62 inclus
- cPanel & WHM versions 11.126.0 jusqu'à 11.126.0.53 inclus
- cPanel & WHM versions 11.130.0 jusqu'à 11.130.0.17 inclus
- cPanel & WHM versions 11.132.0 jusqu'à 11.132.0.28 inclus
- cPanel & WHM versions 11.134.0 jusqu'à 11.134.0.19 inclus
- cPanel & WHM versions 11.136.0 jusqu'à 11.136.0.4 inclus
- WP Squared versions 11.136.1 jusqu'à 11.136.1.6 inclus
- Les versions antérieures à 11.40 ne reçoivent plus de correctif (EOL) et doivent être considérées comme compromises

DÉSCRIPTION :

Il s'agit d'une vulnérabilité de contournement d'authentification dans le flux de connexion et de chargement de session du démon cpsrvd.

cPanel & WHM est un panneau de contrôle d'hébergement web pour serveurs Linux. Il permet la gestion de sites web, de bases de données, de comptes de messagerie et de configurations serveur. WHM fournit l'interface d'administration de niveau racine, tandis que cPanel constitue l'interface utilisateur.

Le mécanisme d'injection CRLF (\r\n) est exploitable via un en-tête d'autorisation Basic malveillant : avant toute authentification, cpsrvd écrit un fichier de session sur le disque sans appeler la fonction de sanitisation filter_sessiondata. Un attaquant peut manipuler le cookie whostmgrsession en omettant un segment attendu pour contourner le chiffrement habituel. Des caractères de saut de ligne bruts sont ainsi injectés dans le fichier de session, permettant l'insertion de propriétés arbitraires telles que user=root.

Elle permet à un attaquant distant non authentifié d'obtenir un accès administrateur complet au panneau de contrôle, avec prise de contrôle totale des sites hébergés, bases de données, configurations serveur et comptes de messagerie.

NB : Un code d'exploitation est disponible en sources ouvertes.

SOLUTION :

Mettre à jour le version « **CPANEL** » (se référer à la documentation).

CONTOURNEMENT PROVISOIRE :

- Bloquer le trafic entrant sur les ports 2083, 2087, 2095 et 2096 au niveau du pare-feu
- Arrêter les services cpsrvd et cpdavd dans l'attente de l'application du correctif

DOCUMENTATION :

Bulletin de sécurité cPanel**:**

- https://support.cpanel.net/hc/en-us/articles/40073787579671-Security-CVE-2026-41940-cPanel-WHM-WP2-Security-Update-04-28-2026