DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 10-05-2026

BULLETIN ALERTES

Object	Vulnérabilités critiques dans cPanel & WHM
Réference	1468
Date de Publication	2026-05-10
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire
- Déni de service
- Traversée de chemin (Path Traversal)

SYSTÉME AFFECTÉ :

- **cPanel & WHM** (toutes les versions non patchées)
- **WP Squared (WP2)**
- Environnements d'hébergement mutualisé (Shared Hosting)

Versions affectées (avant mise à jour) :

- Toutes les versions inférieures à **11.136.0.9**
- Toutes les versions inférieures à **11.134.0.25**
- Toutes les versions inférieures à **11.132.0.31**
- Toutes les versions inférieures à **11.130.0.22**
- Toutes les versions inférieures à **11.126.0.58**
- Toutes les versions inférieures à **11.124.0.37**
- Toutes les versions inférieures à **11.118.0.66**
- Toutes les versions inférieures à **11.110.0.116 / 11.110.0.117**
- Toutes les versions inférieures à **11.102.0.41**
- Toutes les versions inférieures à **11.94.0.30**
- Toutes les versions inférieures à **11.86.0.43**

Cas particulier :

- Serveurs sous **CentOS 6** et **CloudLinux 6** (versions anciennes)

DÉSCRIPTION :

cPanel a divulgué trois vulnérabilités de sécurité critiques répertoriées sous les références **CVE-2026-29201, CVE-2026-29202 et CVE-2026-29203**. Elles affectent son panneau de contrôle d'hébergement très largement déployé, cPanel & WHM, ainsi que la plateforme WP Squared (WP2).

Les trois vulnérabilités nécessitent un accès authentifié. **CVE-2026-29201** permet à un attaquant d'envoyer un chemin relatif via la fonction LOADFEATUREFILE afin de lire n'importe quel fichier sur le serveur (path traversal). **CVE-2026-29202** exploite l'API create_user en injectant du code Perl malveillant dans le paramètre « plugin », entraînant une exécution de code arbitraire (RCE). **CVE-2026-29203** abuse des symlinks : l'attaquant crée un lien symbolique vers un fichier sensible, puis force un chmod via Nova pour modifier ses permissions ou provoquer un déni de service (DoS).

Ces failles exposent les serveurs à des lectures de fichiers arbitraires, à l'injection de code Perl et à des attaques par déni de service.

SOLUTION :

Les administrateurs peuvent mettre à jour immédiatement leur installation cPanel en exécutant le script de mise à jour forcée :

Bash

```
/scripts/upcp --force
```

Une fois l’opération terminée, vérifiez la version installée avec la commande suivante :

Bash

```
/usr/local/cpanel/cpanel -V
```

Confirmez que la version correspond à l’une des versions corrigées mentionnées dans les bulletin d'alerte de l'editeur (section **Documentation**) avant de considérer la remédiation comme terminée.

Étant donné que **CVE-2026-29202** permet une exécution de code directe et que **CVE-2026-29203** ouvre la porte à une escalade de privilèges, ces failles présentent un risque sérieux pour les environnements d’hébergement mutualisé où plusieurs clients partagent un même serveur.

Les fournisseurs d’hébergement utilisant des installations cPanel non corrigées sont fortement exposés à des mouvements latéraux et à une compromission complète du

serveur.

Les administrateurs sont vivement encouragés à appliquer les correctifs disponibles sans délai(se refere la section **Documentation**) et à examiner les logs du serveur à la recherche de tout signe d'activité d'exploitation.

Conseil : La mise à jour se fait simplement via /scripts/upcp --force. Les correctifs sont déjà déployés depuis le 8 mai 2026.

DOCUMENTATION :

- CVE-2026-29201 : https://support.cpanel.net/hc/en-us/articles/40311033698327-Security-CVE-2026-29201-cPanel-WHM-WP2-Security-Update-May-08-2026
- CVE-2026-29202 : https://support.cpanel.net/hc/en-us/articles/40311426610327-Security-CVE-2026-29202-cPanel-WHM-WP2-Security-Update-May-08-2026
- CVE-2026-29203 : https://support.cpanel.net/hc/en-us/articles/40311543760407-Security-CVE-2026-29203-cPanel-WHM-WP2-Security-Update-May-08-2026
- Bulletin d'alerte CVE-2026-29201 : https://support.cpanel.net/hc/en-us/articles/40311033698327
- Bulletin d'alerte CVE-2026-29202 : https://support.cpanel.net/hc/en-us/articles/40311426610327
- Bulletin d'alerte CVE-2026-29203 : https://support.cpanel.net/hc/en-us/articles/40311543760407