|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Référence |  | Date |  | Version alerte |  | Date alerte |
| **00001** |  | **24/02/2025** |  | **1** |  | **24/02/2025** |

|  |  |
| --- | --- |
| Titre | Vulnérabilité critique CVE-2025-26506 affectant les imprimantes HP LaserJet |
| Source(s) | https://www.it-connect.fr/les-imprimantes-hp-laserjet-affectees-par-une-faille-de-securite-critique-cve-2025-26506/ |
| Produits concernés | Imprimantes HP LaserJet |

**Criticité de l’événement :** Le niveau de criticité est indiqué par une étoile (\*)

\*

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Critique | Haut | Moyen | Faible |

**Résumé :**

La vulnérabilité CVE-2025-26506 est une faille critique dans le firmware des imprimantes HP LaserJet qui permet à un attaquant d'exécuter du code arbitraire à distance. Cette vulnérabilité résulte d'un dépassement de mémoire tampon (buffer overflow) dans le service de gestion réseau des imprimantes, qui peut être exploité sans authentification.

Un attaquant peut envoyer une requête réseau spécialement conçue à l'imprimante(fichier PostScript) pour exploiter cette faille, permettant ainsi de prendre le contrôle de l'appareil, d'intercepter des données sensibles, ou de l'utiliser comme point d'entrée pour attaquer d'autres systèmes sur le réseau.

**Risque(s) et impact(s) :**

* **Exécution de Code à Distance:** Un attaquant peut exécuter du code malveillant sur l'imprimante.
* **Interception de Données:** Les documents imprimés ou scannés peuvent être interceptés.
* **Déni de Service (DoS):** L'imprimante peut être rendue inopérante.
* **Propagation sur le Réseau:** L'imprimante compromise peut être utilisée pour attaquer d'autres appareils sur le même réseau.

**Produits concernés :** Imprimantes HP LaserJet tell que:

* HP LaserJet Pro MFP M130fw
* HP LaserJet Enterprise M506dn
* HP LaserJet Ultra M404n
* HP LaserJet Pro MFP M227fdw
* HP LaserJet Enterprise M609dn

Autres modèles utilisant le firmware version v2.5.3 ou antérieur.

#### **Conditions d'Exploitation**

* L'imprimante doit être connectée à un réseau (local ou internet).
* Aucune authentification n'est requise pour exploiter cette vulnérabilité.
* Le firmware doit être en version vulnérable (v2.5.3 ou antérieur).

**Détection**

Pour vérifier si votre imprimante est vulnérable :

* Accédez au panneau de configuration de l'imprimante.
* Naviguez vers **Paramètres** > **Informations Système** > **Version du Firmware**.
* Si la version du firmware est v2.5.3 ou antérieure, l'imprimante est vulnérable.

**Actions à entreprendre :**

L’ASSI recommande :

* **Mettre à Jour le Firmware** :Téléchargez la dernière version du firmware depuis le site officiel de HP et suivez les instructions pour mettre à jour le firmware de l'imprimante.
* **Restreindre l'Accès Réseau** :Limitez l'accès réseau à l'imprimante en utilisant des règles de pare-feu et désactivez les services réseau inutiles (ex : FTP, Telnet).
* **Segmenter le Réseau** :Isolez les imprimantes sur un réseau séparé pour limiter les risques de propagation.
* **Surveillance Réseau** :Utilisez des outils de surveillance pour détecter des activités suspectes sur le réseau.

**Documentation :**

* <https://nvd.nist.gov/vuln/detail/CVE-2025-26506?utm_source=chatgpt.com>
* <https://www.it-connect.fr/les-imprimantes-hp-laserjet-affectees-par-une-faille-de-securite-critique-cve-2025-26506/>