



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant des imprimantes HP
Numéro de Référence	41140504/23
Date de publication	05 Avril 2023
Risque	Important
Impact	Critique

Systèmes affectés

- HP Color LaserJet Enterprise M455
- HP Color LaserJet Enterprise MFP M480
- HP Color LaserJet Managed E45028
- HP Color LaserJet Managed MFP E47528
- HP Color LaserJet Managed MFP E785dn, HP Color LaserJet Managed MFP E78523, E78528
- HP Color LaserJet Managed MFP E786, HP Color LaserJet Managed Flow MFP E786, HP Color LaserJet Managed MFP E78625/30/35, HP Color LaserJet Managed Flow MFP E78625/30/35
- HP Color LaserJet Managed MFP E877, E87740/50/60/70, HP Color LaserJet Managed Flow E87740/50/60/70
- HP LaserJet Enterprise M406
- HP LaserJet Enterprise M407
- HP LaserJet Enterprise MFP M430
- HP LaserJet Enterprise MFP M431
- HP LaserJet Managed E40040
- HP LaserJet Managed MFP E42540
- HP LaserJet Managed MFP E730, HP LaserJet Managed MFP E73025, E73030
- HP LaserJet Managed MFP E731, HP LaserJet Managed Flow MFP M731, HP LaserJet Managed MFP E73130/35/40, HP LaserJet Managed Flow MFP E73130/35/40
- HP LaserJet Managed MFP E826dn, HP LaserJet Managed Flow MFP E826z, HP LaserJet Managed E82650/60/70, HP LaserJet Managed E82650/60/70

Identificateurs externes

- CVE-2023-1707

Bilan de la vulnérabilité

HP annonce la correction d'une vulnérabilité critique affectant certaines de ses imprimantes. Cette vulnérabilité est exploitable si le protocole IPsec et la fonctionnalité FutureSmart sont activés et elle permet à un attaquant d'accéder à des informations confidentielles.

Solution

Aucune mise à jour n'est disponible pour le moment. Cependant, si vous utilisez la version 5.6 de FutureSmart, il est recommandé de la rétrograder vers la version 5.5.0.3

Risque

- Accès à des données confidentielles

Références

Bulletin de sécurité de de HP :

- https://support.hp.com/us-en/document/ish_7905330-7905358-16/hpsbpi03838