AVIS DE SECURITE

Objet	**Vulnérabilité exploitée dans Ivanti Connect Secure et multiples vulnérabilités dans les produits Ivanti (CVE-2026-104935)**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-261
TLP	WHITE

Résumé

Ivanti a publié le 13/10/2026 ses correctifs de sécurité d'octobre. La vulnérabilité CVE-2026-104935 (CVSS v3.1 : 8.6), un contournement d'authentification dans Ivanti Connect Secure, permet à un attaquant distant non authentifié d'exécuter des commandes arbitraires ; son exploitation active est signalée par l'éditeur et elle a été ajoutée au catalogue CISA KEV le 13/10/2026. Des vulnérabilités sont également corrigées dans Ivanti Neurons Patch for Intune et Ivanti Xtraction.

Risque de sécurité

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

Systèmes affectés

- Ivanti Connect Secure (ICS) 22.8Rx antérieures à 22.8R2.5
- Ivanti Connect Secure (ICS) 25.1.1.x antérieures à 25.1.1.2
- Ivanti Connect Secure (ICS) 25.1.3.x antérieures à 25.1.3.1
- Ivanti Xtraction versions antérieures à 2026.4
- Ivanti Neurons Patch for Intune (correctif appliqué automatiquement le 16/09/2026)

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 13/10/2026 :
   - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935
   - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-Patch-for-Intune-October-2026
   - https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Xtraction-Multiple-CVEs
2. Mettre à jour Ivanti Connect Secure vers une version corrigée sans délai et exécuter l'Integrity Checker Tool
3. Mettre à jour Ivanti Xtraction vers la version 2026.4 ou ultérieure