



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant Ivanti Connect Secure, Policy Secure et Secure Access Client
Numéro de Référence	52621202/25
Date de Publication	12 Février 2025
Risque	Critique
Impact	Critique

Systemes affectés

- Ivanti Connect Secure versions antérieures à 22.7R2.6
- Ivanti Policy Secure 22.7R1.3
- Ivanti Secure Access Client versions antérieures à 22.8R1

Identificateurs externes

CVE-2024-10644 CVE-2024-12058 CVE-2024-13813 CVE-2024-13830
CVE-2024-13842 CVE-2024-13843 CVE-2024-38657 CVE-2025-22467

Bilan de la vulnérabilité

Ivanti a publié des mises à jour de sécurité qui permettent de corriger plusieurs vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant non authentifié d'exécuter du code arbitraire, d'élever ses privilèges ou d'accéder à des données confidentielles.

Solution

Veillez se référer au bulletin de sécurité d'Ivanti pour l'obtention des correctifs.

Risque

- Exécution de code arbitraire
- Elévation de privilèges
- Accès à des données confidentielles

Référence

Bulletin de sécurité d'Ivanti:

https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs?language=en_US