aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité dans Ivanti

2024-01-11 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

IVANTI

Ivanti a publié un bulletin de sécurité le 10 janvier 2024 concernant deux vulnérabilités qui affectent *Ivanti Connect Secure* (ICS) et *Ivanti Policy Secure gateways*.

CVE-2024-21887

Une vulnerabilité de type injection de commande dans les composants web d'*Ivanti Connect Secure* et *Ivanti Policy Secure* a été découverte par des chercheurs en sécurité de Volexity.

L'exploitation de cette vulnérabilité par un attaquant distant et authentifié permet, en envoyant une requête spécifiquement forgée, d'éxecuter du code arbitraire.

La CVE-2024-21887 (exécution de code arbitraire) peut être exploitée conjointement avec la CVE-2023-46805 (contournement d'authentification).

Volexity a observé l'exploitation de cette vulnérabilité et l'a attribué au groupe UTA0178.
Le CISA a intégré cette vulnérabilité dans sa base de données *Known Exploited Vulnerabilities (KEV)* le 10 janvier 2024.

Type de vulnérabilité

- **CWE-77** : Improper Neutralization of Special Elements used in a Command ('Command Injection')

Risques

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Élevé	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Preuve de concept

Aucune preuve de concept n'est disponible en source ouverte.

CVE-2023-46805

Un défaut de vérification d'authentification dans les composants web d'*Ivanti Connect Secure* et *Ivanti Policy Secure* a été découvert par des chercheurs en sécurité de Volexity.

L'exploitation de cette vulnérabilité par un attaquant distant et non authentifié permet, en contournant les contrôles de sécurité, d'accéder aux informations du service web.

Volexity a observé l'exploitation de cette vulnérabilité et l'a attribué au groupe UTA0178.
Le CISA a intégré cette vulnérabilité dans sa base de données *Known Exploited Vulnerabilities (KEV)* le 10 janvier 2024.

Type de vulnérabilité

- **CWE-287** : Improper Authentication

Risques

- Contournement de la politique de sécurité

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Faible
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Aucun

Preuve de concept

Aucune preuve de concept n'est disponible en source ouverte.

Produits impactés

- Ivanti Connect Secure Ivanti Policy Secure gateways version 9.x jusqu'à 22.x

Recommandations

- Il n'existe pas encore de correctif proposé par l'éditeur. Une première version devrait être mise à la disposition à compter du 22 janvier et la version finale à compter du 19 février.
- Ivanti propose une solution de contournement en important le fichier *mitigation.release.20240107.1.xml* via son portail de téléchargement. La procédure à suivre pour l'installation de cette solution de contournement est disponible sur leur article KB.
- Des informations complémentaires sont disponibles dans le bulletin Ivanti.

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	IP	206.189.208[.]156	Addresse IP attribuée à UTA0178
TLP:CLEAR	Domaine	gpoaccess[.]com	Domaine suspect attribué à UTA0178
TLP:CLEAR	Domaine	webb-institute[.]com	Domaine suspect attribué à UTA0178
TLP:CLEAR	IP	75.145.243[.]85	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	47.207.9[.]89	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	98.160.48[.]170	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	173.220.106[.]166	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	73.128.178[.]221	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	50.243.177[.]161	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	50.213.208[.]89	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	64.24.179[.]210	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	75.145.224[.]109	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	50.215.39[.]49	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	71.127.149[.]194	Addresse IP attribuée à UTA0178
TLP:CLEAR	IP	173.53.43[.]7	Addresse IP attribuée à UTA0178

Références

Ivanti

- https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-policy-secure-gateways
- https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

CVE-2024-21887

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21887

CVE-2023-46805

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46805