aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité dans Ivanti

2024-02-16 | **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*.

Mise à jour du 31 janvier 2024 : Ivanti a mis à jour son bulletin de sécurité concernant la découverte de deux nouvelles vulnérabilités (CVE-2024-21888 et CVE-2024-21893) affectant *Ivanti Neurons pour ZTA*, *Ivanti Connect Secure* (ICS) et *Ivanti Policy Secure gateways*.

Mise à jour du 02 février 2024 : Pour faciliter la lecture des recommandations de l'éditeur, ces dernières ont été mises à jour dans la rubrique idoine.

Mise à jour du 12 février 2024 : Mise à jour et ajout d'Indicateurs de Compromissions (IoCs).

Mise à jour du 16 février 2024 : Ivanti a publié de nouveaux correctifs pour Ivanti Connect Secure, Ivanti Policy Secure et Ivanti Neurons for ZTA.

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 APT UTA0178.
Le CISA a intégré cette vulnérabilité dans sa base de données *Known Exploited Vulnerabilities (KEV)* le 10 janvier 2024. Mise à jour du 12 janvier 2024: Le 11 janvier 2024, le CERT-FR a alerté sur l'exploitation de la CVE-2024-21887.
Le même jour Mandiant a publié un rapport précisant l'exploitation des ces vulnérabilités accompagné de nouveaux indicateurs de compromissions ainsi que des règles de détection.
Mise à jour du 22 janvier 2024 : Ivanti a apporté la preuve de nouvelles exploitations de ces vulnérabilités, ainsi que de nouveaux indicateurs de compromission.

Mise à jour du 12 janvier 2024: Le rapport de Mandiant met en exergue l'emploi de logiciels malveillants pendant et après l'exploitation des deux vulnérabilités. Ces maliciels ont notamment permis aux attaquants de garantir leur persistence, de contourner les dispositifs de détection, de dérober des idenfiants et mots de passe sur les systèmes compromis.

Type de vulnérabilité

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

Risque

- 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

Produits impactés

- Ivanti Connect Secure Ivanti Policy Secure versions 9.x et 22.x

Recommandations

Mise à jour du 16 février 2024 :

- Mettre à jour Ivanti Connect Secure vers la version 9.1R14.5, 9.1R15.3, 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.1R6.1, 22.3R1.1, 22.2R4.1, 22.4R1.1, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2 ou ultérieure.
- Mettre à jour Ivanti Policy Secure vers la version : 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.4R1.1, 22.5R1.2, 22.6R1.1 ou ultérieure.
- Avant d'appliquer les correctifs, Ivanti recommande de s'assurer de l'intégrité des équipements concernés. Pour cela, un outil a été mis à disposition par l'éditeur, *Ivanti integrity checker, ICT*. Concernant les équipements compromis, une procédure de rémédiation a été publiée dans le bulletin d'Ivanti.
- L'éditeur recommande également de réinitialiser les appareils avant de déployer les mises à jours afin d'empêcher les attaquants de maintenir une persistance lors de la mise à niveau. Ainsi que de changer tous les mots de passe (utilisateurs, administrateurs), les clés API et de renouveller les certificats déployés sur les équipements.
- Si le correctif ne peut pas être déployé, il est nécessaire de mettre en place la solution de contournement en important le fichier *mitigation.release.20240107.1.xml* via son portail de téléchargement. La procédure associée est disponible sur leur article KB.
- Des informations complémentaires sont disponibles dans le bulletin Ivanti.

Preuve de concept

Mise à jour du 22 janvier 2024 : Une preuve de concept est disponible en sources ouvertes.

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 APT UTA0178.
Le CISA a intégré cette vulnérabilité dans sa base de données *Known Exploited Vulnerabilities (KEV)* le 10 janvier 2024.
Mise à jour du 12 janvier 2024: Le 11 janvier 2024, le CERT-FR a alerté sur l'exploitation de la CVE-2023-46805.
Le même jour Mandiant a publié un rapport concernant l'exploitation des ces vulnérabilités accompagné de nouveaux indicateurs de compromissions ainsi que des règles de détection.
Mise à jour du 22 janvier 2024 : Ivanti a apporté la preuve de nouvelles exploitations de ces vulnérabilités, ainsi que de nouveaux indicateurs de compromission.

Mise à jour du 12 janvier 2024: Plusieurs logiciels malveillants utilisés pendant et après l'exploitation des CVE-2023-46805 et CVE-2024-21887 ont été identifiés par les chercheurs de Mandiant. Ces maliciels ont notamment permis aux attaquants de garantir leur persistence, de contourner les dispositifs de détection, de dérober des idenfiants et mots de passe sur les systèmes compromis.

Type de vulnérabilité

- **CWE-287** : Improper Authentication

Risque

- 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

Produits impactés

- Ivanti Connect Secure et Ivanti Policy Secure versions 9.x et 22.x

Recommandations

Mise à jour du 16 février 2024 :

- Mettre à jour Ivanti Connect Secure vers la version 9.1R14.5, 9.1R15.3, 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.1R6.1, 22.3R1.1, 22.2R4.1, 22.4R1.1, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2 ou ultérieure.
- Mettre à jour Ivanti Policy Secure vers la version : 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.4R1.1, 22.5R1.2, 22.6R1.1 ou ultérieure.
- Avant d'appliquer les correctifs, Ivanti recommande de s'assurer de l'intégrité des équipements concernés. Pour cela, un outil a été mis à disposition par l'éditeur, *Ivanti integrity checker, ICT*. Concernant les équipements compromis, une procédure de rémédiation a été publiée dans le bulletin d'Ivanti.
- L'éditeur recommande également de réinitialiser les appareils avant de déployer les mises à jours afin d'empêcher les attaquants de maintenir une persistance lors de la mise à niveau. Ainsi que de changer tous les mots de passe (utilisateurs, administrateurs), les clés API et de renouveller les certificats déployés sur les équipements.
- Si le correctif ne peut pas être déployé, il est nécessaire de mettre en place la solution de contournement en important le fichier *mitigation.release.20240107.1.xml* via son portail de téléchargement. La procédure associée est disponible sur leur article KB.
- Des informations complémentaires sont disponibles dans le bulletin Ivanti.

Preuve de concept

Mise à jour du 22 janvier 2024 : Une preuve de concept est disponible en sources ouvertes.

Mise à jour du 31 janvier 2024 :

CVE-2024-21893

Une vulnérabilité de type « Server-Side Request Forgery » dans le composant SAML d'Ivanti permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, de porter atteinte à la confidentialité.

La vulnérabilité est exploitée.

Type de vulnérabilité

- **CWE-918** : Server-Side Request Forgery (SSRF)

Risque

- Atteinte à la confidentialité des données

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

Produits impactés

- Ivanti Connect Secure et Ivanti Policy Secure versions 9.x et 22.x
- Ivanti Neurons pour ZTA

Recommandations

Mise à jour du 16 février 2024 :

- Mettre à jour Ivanti Connect Secure vers la version 9.1R14.5, 9.1R15.3, 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.1R6.1, 22.3R1.1, 22.2R4.1, 22.4R1.1, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2 ou ultérieure.
- Mettre à jour Ivanti Policy Secure vers la version : 9.1R16.3, 9.1R17.3, 9.1R18.4, 22.4R1.1, 22.5R1.2, 22.6R1.1 ou ultérieure.
- Mettre à jour ZTA gateways vers la version 22.5R1.6, 22.6R1.5, 22.6R1.7 ou ultérieure.
- Avant d'appliquer les correctifs, Ivanti recommande de s'assurer de l'intégrité des équipements concernés. Pour cela, un outil a été mis à disposition par l'éditeur, *Ivanti integrity checker, ICT*. Concernant les équipements compromis, une procédure de rémédiation a été publiée dans le bulletin d'Ivanti.
- L'éditeur recommande également de réinitialiser les appareils avant de déployer les mises à jours afin d'empêcher les attaquants de maintenir une persistance lors de la mise à niveau. Ainsi que de changer tous les mots de passe (utilisateurs, administrateurs), les clés API et de renouveller les certificats déployés sur les équipements.
- Si le correctif ne peut pas être déployé, il est nécessaire de mettre en place la solution de contournement en important le fichier *mitigation.release.20240107.1.xml* via son portail de téléchargement. La procédure associée est disponible sur leur article KB.

- Des informations complémentaires sont disponibles dans le bulletin Ivanti.

Preuve de concept

Mise à jour du 12 février 2024 : Une preuve de concept est disponible en sources ouvertes.

Règles Yara (Détection)

Backdoor ZIPLINE

```
rule M_Hunting_Backdoor_ZIPLINE_1 {
  meta:
    author = "Mandiant"
    description = "This rule detects unique strings in ZIPLINE, a passive ELF backdoor that waits for
incoming TCP connections to receive commands from the threat actor."
  strings:
    $s1 = "SSH-2.0-OpenSSH_0.3xx" ascii
    $s2 = "$(exec $installer $@)" ascii
    $t1 = "./installer/do-install" ascii
    $t2 = "./installer/bom_files/" ascii
    $t3 = "/tmp/data/root/etc/ld.so.preload" ascii
    $t4 = "/tmp/data/root/home/etc/manifest/exclusion_list" ascii
  condition:
    uint32(0) == 0x464c457f and
    filesize < 5MB and
    ((1 of ($s*)) or
    (3 of ($t*)))
}
```

Dropper WIREFIRE

```
rule M_Hunting_Dropper_WIREFIRE_1 {
  meta:
    author = "Mandiant"
    description = "This rule detects WIREFIRE, a web shell written in Python that exists as trojanized logic
to a component of the pulse secure appliance."
    md5 = "6de651357a15efd01db4e658249d4981"
  strings:
    $s1 = "zlib.decompress(aes.decrypt(base64.b64decode(" ascii
    $s2 = "aes.encrypt(t+('\\x00'*(16-len(t)%16))" ascii
    $s3 = "Handles DELETE request to delete an existing visits data." ascii
    $s4 = "request.data.decode().startswith('GIF'):" ascii
    $s5 = "Utils.api_log_admin" ascii
  condition:
    filesize < 10KB
    and all of them
}
```

Des règles Yara supplémentaires sont disponibles sur les bulletins Mandiant et Volexity.

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	Domaine	gpoaccess[.]com	Domaine suspect attribué à UTA0178
TLP:CLEAR	Domaine	webb-institute[.]com	Domaine suspect attribué à UTA0178
TLP:CLEAR	Domaine	symantke[.]com	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	miltonhouse[.]nl	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	entraide-internationale[.]fr	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	api.d-n-s[.]name	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	cpanel.netbar[.]org	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	clickcom[.]click	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	clicko[.]click	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	duorhytm[.]fun	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	line-api[.]com	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	areekaweb[.]com	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	ehangmun[.]com	Serveur C2 WARPWIRE
TLP:CLEAR	Domaine	secure-cama[.]com	Serveur C2 WARPWIRE
TLP:CLEAR	URL	103.233.11[.]5:1999/doc	URL utilisée pour télécharger des charges utiles
TLP:CLEAR	URL	45.130.22[.]219/ivanti.js	URL utilisée pour télécharger des charges utiles
TLP:CLEAR	URL	45.130.22[.]219/ivanti	URL utilisée pour télécharger des charges utiles
TLP:CLEAR	URL	137.220.130[.]2/doc	URL utilisée pour télécharger des charges utiles
TLP:CLEAR	URL	124.156.132[.]142:6999/python	URL utilisée pour télécharger des charges utiles
TLP:CLEAR	URL	raw.githubusercontent[.]com/momika233/test/main/m.sh	URL utilisée pour télécharger des charges utiles
TLP:CLEAR	URL	github[.]com/momika233/test/raw/main/watchbog	URL utilisée pour télécharger watchbog
TLP:CLEAR	URL	github[.]com/momika233/test/raw/main/watchd0g	URL utilisée pour télécharger watchd0g
TLP:CLEAR	IP	206.189.208[.]156	Adresse IP attribuée à UTA0178 (Hébergeur, risque de faux positifs)
TLP:CLEAR	IP	75.145.243[.]85	Adresse IP attribuée à UTA0178
TLP:CLEAR	IP	47.207.9[.]89	Adresse IP attribuée à UTA0178 tied to Cyberoam proxy network
TLP:CLEAR	IP	98.160.48[.]170	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	173.220.106[.]166	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	73.128.178[.]221	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	50.243.177[.]161	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	50.213.208[.]89	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	64.24.179[.]210	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	75.145.224[.]109	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	IP	50.215.39[.]49	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	71.127.149[.]194	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	173.53.43[.]7	Adresse IP attribuée à UTA0178 associée à Cyberoam proxy network
TLP:CLEAR	IP	146.0.228[.]66	Serveur C2 WARPWIRE
TLP:CLEAR	IP	159.65.130[.]146	Serveur C2 WARPWIRE (Hébergeur, risque de faux positifs)
TLP:CLEAR	IP	8.137.112[.]245	Serveur C2 WARPWIRE (Hébergeur, risque de faux positifs)
TLP:CLEAR	IP	91.92.254[.]14	Serveur C2 WARPWIRE
TLP:CLEAR	IP	186.179.39[.]235	Exploitation massive
TLP:CLEAR	IP	45.61.136[.]14	Activités post-exploitation
TLP:CLEAR	IP	138.68.61[.]82	IPs contactée pour télécharger les charges utiles (Hébergeur, risque de faux positifs)
TLP:CLEAR	IP	192.252.183[.]116	IPs contactée pour télécharger les charges utiles
TLP:CLEAR	IP	141.98.7[.]6	IPs contactée pour télécharger les charges utiles (Hébergeur, risque de faux positifs)
TLP:CLEAR	IP	103.215.77[.]51	IPs contactée pour télécherger les charges utiles
TLP:CLEAR	IP	45.152.66[.]151	IPs contactée pour télécharger les charges utiles (Hébergeur, risque de faux positifs)
TLP:CLEAR	MD5 I Filename	3045f5b3d355a9ab26ab6f44cc831a83 I health.py	CHAINLINE Web Shell
TLP:CLEAR	MD5 I Filename	3d97f55a03ceb4f71671aa2ecf5b24e9 I compcheckresult.cgi	LIGHTWIRE Web Shell
TLP:CLEAR	MD5 I Filename	2ec505088b942c234f39a37188e80d7a I lastauthserverused.js	WARPWIRE permet de dérober les identifiants
TLP:CLEAR	MD5 I Filename	8eb042da6ba683ef1bae460af103cc44 I lastauthserverused.js	WARPWIRE permet de dérober les identifiants
TLP:CLEAR	MD5 I Filename	a739bd4c2b9f3679f43579711448786f I lastauthserverused.js	WARPWIRE permet de dérober les identifiants
TLP:CLEAR	MD5 I Filename	a81813f70151a022ea1065b7f4d6b5ab I lastauthserverused.js	WARPWIRE permet de dérober les identifiants
TLP:CLEAR	MD5 I Filename	d0c7a334a4d9dcd3c6335ae13bee59ea I lastauthserverused.js	WARPWIRE permet de dérober les identifiants
TLP:CLEAR	MD5 I Filename	e8489983d73ed30a4240a14b1f161254 I lastauthserverused.js	WARPWIRE permet de dérober les identifiants
TLP:CLEAR	MD5 I Filename	465600cece80861497e8c1c86a07a23e I category.py	Web Shell FRAMESTING
TLP:CLEAR	MD5 I Filename	65f19b39dc43f202a6d26223d0472b66 I watchd0g	Backdoor KrustyLoader développée en Go
TLP:CLEAR	SHA1 I Filename	46e0847be3dab555790446f267e2c2aea5a3b9bb I watchd0g	Backdoor KrustyLoader développée en Go
TLP:CLEAR	SHA256 I Filename	1e1e94bd2bfd5054265123bf55c4cf6ce87de6692d9329bda4a37e89272356e4 I watchd0g	Backdoor KrustyLoader développée en Go

TLP	TYPE	VALEUR	COMMENTAIRE
TLP:CLEAR	MD5 I Filename	03356c7fac38d09b0d07873f0d3f2b37 I watchbog	Malware watchbog développé en Go
TLP:CLEAR	SHA1 I Filename	2a76d2d4bef67d565c331fc6945724d31bdf989c I watchbog	Malware watchbog développé en Go
TLP:CLEAR	SHA256 I Filename	8eadb5beeb21d4a95dacd133cb2b934342fcb39fe4df2a8387a0d5499c72450d I watchbog	Malware watchbog développé en Go
TLP:CLEAR	SHA256 I Filename	cf20940907be484440e8343aa05505ad2e4d6d1f24ef29504bfa54ade4a8455f I m.sh	Dropper de watchbog et watchd0g
TLP:CLEAR	Filename	visits.py	WIREFIRE Web Shell
TLP:CLEAR	Filename	sessionserver.sh	THINSPOOL Web Shell dropper
TLP:CLEAR	Filename	sessionserver.pl	THINSPOOL Utility Script
TLP:CLEAR	Filename	libsecure.so.1	ZIPLINE Backdoor

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/
- https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-001/
- https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US
- https://www.cisa.gov/news-events/alerts/2024/01/19/cisa-issues-emergency-directive-ivanti-vulnerabilities
- https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation
- https://unit42.paloaltonetworks.com/threat-brief-ivanti-cve-2023-46805-cve-2024-21887/
- https://www.greynoise.io/blog/ivanti-connect-secure-exploited-to-install-cryptominers

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

CVE-2024-21893

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21893