Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N

Agence nationale
de la sécurité des
systèmes d'information

Paris, le 13 novembre 2024
N° CERTFR-2024-AVI-0967

Affaire suivie par: CERT-FR

AVIS DU CERT-FR

Objet: Multiples vulnérabilités dans les produits Ivanti

GESTION DU DOCUMENT

Référence	CERTFR-2024-AVI-0967
Titre	Multiples vulnérabilités dans les produits Ivanti
Date de la première version	13 novembre 2024
Date de la dernière version	13 novembre 2024

Source(s)	Bulletin de sécurité Ivanti 000095993 du 12 novembre 2024 Bulletin de sécurité Ivanti 000096001 du 12 novembre 2024 Bulletin de sécurité Ivanti november-2024-security-update du 12 novembre 2024

Une gestion de version détaillée se trouve à la fin de ce document.

RISQUES

- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire à distance
- Injection de code indirecte à distance (XSS)
- Élévation de privilèges

SYSTÈMES AFFECTÉS

- Connect Secure (ICS) versions antérieures à 22.7R2.3
- Endpoint Manager (EPM) 2022 versions antérieures à SU6 sans le correctif de sécurité de novembre
- Endpoint Manager (EPM) 2024 sans le correctif de sécurité de novembre
- Policy Secure (IPS) versions antérieures à 22.7R1.2
- Secure Access Client (ISAC) versions antérieures à 22.7R4

RÉSUMÉ

De multiples vulnérabilités ont été découvertes dans les produits Ivanti. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance.

SOLUTIONS

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION

- Bulletin de sécurité Ivanti 000095993 du 12 novembre 2024
  https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs (https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs)
- Bulletin de sécurité Ivanti 000096001 du 12 novembre 2024
  https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022 (https://forums.ivanti.com/s/article/Security-Advisory-EPM-November-2024-for-EPM-2024-and-EPM-2022)
- Bulletin de sécurité Ivanti november-2024-security-update du 12 novembre 2024
  https://www.ivanti.com/blog/november-2024-security-update (https://www.ivanti.com/blog/november-2024-security-update)
- Référence CVE CVE-2024-11004
  https://www.cve.org/CVERecord?id=CVE-2024-11004 (https://www.cve.org/CVERecord?id=CVE-2024-11004)
- Référence CVE CVE-2024-11005
  https://www.cve.org/CVERecord?id=CVE-2024-11005 (https://www.cve.org/CVERecord?id=CVE-2024-11005)
- Référence CVE CVE-2024-11006
  https://www.cve.org/CVERecord?id=CVE-2024-11006 (https://www.cve.org/CVERecord?id=CVE-2024-11006)
- Référence CVE CVE-2024-11007
  https://www.cve.org/CVERecord?id=CVE-2024-11007 (https://www.cve.org/CVERecord?id=CVE-2024-11007)

- Référence CVE CVE-2024-29211
  https://www.cve.org/CVERecord?id=CVE-2024-29211 (https://www.cve.org/CVERecord?id=CVE-2024-29211)
- Référence CVE CVE-2024-32839
  https://www.cve.org/CVERecord?id=CVE-2024-32839 (https://www.cve.org/CVERecord?id=CVE-2024-32839)
- Référence CVE CVE-2024-32841
  https://www.cve.org/CVERecord?id=CVE-2024-32841 (https://www.cve.org/CVERecord?id=CVE-2024-32841)
- Référence CVE CVE-2024-32844
  https://www.cve.org/CVERecord?id=CVE-2024-32844 (https://www.cve.org/CVERecord?id=CVE-2024-32844)
- Référence CVE CVE-2024-32847
  https://www.cve.org/CVERecord?id=CVE-2024-32847 (https://www.cve.org/CVERecord?id=CVE-2024-32847)
- Référence CVE CVE-2024-34780
  https://www.cve.org/CVERecord?id=CVE-2024-34780 (https://www.cve.org/CVERecord?id=CVE-2024-34780)
- Référence CVE CVE-2024-34781
  https://www.cve.org/CVERecord?id=CVE-2024-34781 (https://www.cve.org/CVERecord?id=CVE-2024-34781)
- Référence CVE CVE-2024-34782
  https://www.cve.org/CVERecord?id=CVE-2024-34782 (https://www.cve.org/CVERecord?id=CVE-2024-34782)
- Référence CVE CVE-2024-34784
  https://www.cve.org/CVERecord?id=CVE-2024-34784 (https://www.cve.org/CVERecord?id=CVE-2024-34784)
- Référence CVE CVE-2024-34787
  https://www.cve.org/CVERecord?id=CVE-2024-34787 (https://www.cve.org/CVERecord?id=CVE-2024-34787)
- Référence CVE CVE-2024-37376
  https://www.cve.org/CVERecord?id=CVE-2024-37376 (https://www.cve.org/CVERecord?id=CVE-2024-37376)
- Référence CVE CVE-2024-37398

https://www.cve.org/CVERecord?id=CVE-2024-37398 (https://www.cve.org/CVERecord?id=CVE-2024-37398)

- Référence CVE CVE-2024-37400
  https://www.cve.org/CVERecord?id=CVE-2024-37400 (https://www.cve.org/CVERecord?id=CVE-2024-37400)
- Référence CVE CVE-2024-38649
  https://www.cve.org/CVERecord?id=CVE-2024-38649 (https://www.cve.org/CVERecord?id=CVE-2024-38649)
- Référence CVE CVE-2024-38654
  https://www.cve.org/CVERecord?id=CVE-2024-38654 (https://www.cve.org/CVERecord?id=CVE-2024-38654)
- Référence CVE CVE-2024-38655
  https://www.cve.org/CVERecord?id=CVE-2024-38655 (https://www.cve.org/CVERecord?id=CVE-2024-38655)
- Référence CVE CVE-2024-38656
  https://www.cve.org/CVERecord?id=CVE-2024-38656 (https://www.cve.org/CVERecord?id=CVE-2024-38656)
- Référence CVE CVE-2024-39709
  https://www.cve.org/CVERecord?id=CVE-2024-39709 (https://www.cve.org/CVERecord?id=CVE-2024-39709)
- Référence CVE CVE-2024-39710
  https://www.cve.org/CVERecord?id=CVE-2024-39710 (https://www.cve.org/CVERecord?id=CVE-2024-39710)
- Référence CVE CVE-2024-39711
  https://www.cve.org/CVERecord?id=CVE-2024-39711 (https://www.cve.org/CVERecord?id=CVE-2024-39711)
- Référence CVE CVE-2024-39712
  https://www.cve.org/CVERecord?id=CVE-2024-39712 (https://www.cve.org/CVERecord?id=CVE-2024-39712)
- Référence CVE CVE-2024-47905
  https://www.cve.org/CVERecord?id=CVE-2024-47905 (https://www.cve.org/CVERecord?id=CVE-2024-47905)
- Référence CVE CVE-2024-47906
  https://www.cve.org/CVERecord?id=CVE-2024-47906 (https://www.cve.org/CVERecord?id=CVE-2024-47906)

- Référence CVE CVE-2024-47907
  https://www.cve.org/CVERecord?id=CVE-2024-47907 (https://www.cve.org/CVERecord?id=CVE-2024-47907)
- Référence CVE CVE-2024-47909
  https://www.cve.org/CVERecord?id=CVE-2024-47909 (https://www.cve.org/CVERecord?id=CVE-2024-47909)
- Référence CVE CVE-2024-50322
  https://www.cve.org/CVERecord?id=CVE-2024-50322 (https://www.cve.org/CVERecord?id=CVE-2024-50322)
- Référence CVE CVE-2024-50323
  https://www.cve.org/CVERecord?id=CVE-2024-50323 (https://www.cve.org/CVERecord?id=CVE-2024-50323)
- Référence CVE CVE-2024-50324
  https://www.cve.org/CVERecord?id=CVE-2024-50324 (https://www.cve.org/CVERecord?id=CVE-2024-50324)
- Référence CVE CVE-2024-50326
  https://www.cve.org/CVERecord?id=CVE-2024-50326 (https://www.cve.org/CVERecord?id=CVE-2024-50326)
- Référence CVE CVE-2024-50327
  https://www.cve.org/CVERecord?id=CVE-2024-50327 (https://www.cve.org/CVERecord?id=CVE-2024-50327)
- Référence CVE CVE-2024-50328
  https://www.cve.org/CVERecord?id=CVE-2024-50328 (https://www.cve.org/CVERecord?id=CVE-2024-50328)
- Référence CVE CVE-2024-50329
  https://www.cve.org/CVERecord?id=CVE-2024-50329 (https://www.cve.org/CVERecord?id=CVE-2024-50329)
- Référence CVE CVE-2024-50330
  https://www.cve.org/CVERecord?id=CVE-2024-50330 (https://www.cve.org/CVERecord?id=CVE-2024-50330)
- Référence CVE CVE-2024-7571
  https://www.cve.org/CVERecord?id=CVE-2024-7571 (https://www.cve.org/CVERecord?id=CVE-2024-7571)
- Référence CVE CVE-2024-8495

https://www.cve.org/CVERecord?id=CVE-2024-8495 (https://www.cve.org/CVERecord?id=CVE-2024-8495)

- Référence CVE CVE-2024-8539
  https://www.cve.org/CVERecord?id=CVE-2024-8539 (https://www.cve.org/CVERecord?id=CVE-2024-8539)
- Référence CVE CVE-2024-9420
  https://www.cve.org/CVERecord?id=CVE-2024-9420 (https://www.cve.org/CVERecord?id=CVE-2024-9420)
- Référence CVE CVE-2024-9842
  https://www.cve.org/CVERecord?id=CVE-2024-9842 (https://www.cve.org/CVERecord?id=CVE-2024-9842)
- Référence CVE CVE-2024-9843
  https://www.cve.org/CVERecord?id=CVE-2024-9843 (https://www.cve.org/CVERecord?id=CVE-2024-9843)

GESTION DÉTAILLÉE DU DOCUMENT

le 13 novembre 2024

Version initiale