



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Cisco
Numéro de Référence	40050202/23
Date de Publication	02 Février 2023
Risque	Important
Impact	Important

Systemes affectés

- Cisco IOx Application Hosting Environment
- Cisco Prime Infrastructure
- Cisco Identity Services Engine
- Cisco Identity Services Engine
- Cisco RV340, RV340W, RV345, et RV345P Dual WAN Gigabit VPN Routers

Identificateurs externes

- CVE-2023-20076, CVE-2023-20068, CVE-2023-20030, CVE-2023-20021, CVE-2023-20022, CVE-2023-20023, CVE-2023-20073

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Cisco susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 01 Février 2023 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Déni de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletins de sécurité Cisco du 01 Février 2023:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-pi-xss-PU6dnfD9>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-GecEHY58>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-os-injection-pxhKsDM>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-afu-EXxwA65V>