



## BULLETIN DE SECURITE

|                            |  |
|----------------------------|--|
| <b>Titre</b>               | Vulnérabilités dans les produits Cisco |
| <b>Numéro de Référence</b> | 44000210/23                            |
| <b>Date de Publication</b> | 02 Octobre 2023                        |
| <b>Risque</b>              | Important                              |
| <b>Impact</b>              | Important                              |

### Systemes affectés

- Cisco Catalyst SD-WAN Manager (anciennement Cisco SD-WAN vManage) versions antérieures à 20.12.1
- Cisco IOS et IOS XE sans le dernier correctif de sécurité (vérifier sur le site de l'éditeur pour identifier les versions vulnérables)
- Cisco DNA Center versions antérieures à 2.3.5.4
- Cisco DNA Center versions 2.3.6.x antérieures à 2.3.7.0
- Cisco IOS et IOS XE avec le protocole GDOI ou G-IKEv2 activé

### Identificateurs externes

- CVE-2023-20135, CVE-2023-20236, CVE-2023-20233, CVE-2023-20191, CVE-2023-20190,

### Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Cisco susmentionnés. Un attaquant pourrait exploiter ces failles afin de causer un déni de service, contourner la politique de sécurité ou exécuter du code arbitraire à distance.

### Solution

Veillez se référer au bulletin de sécurité Cisco du 27 Septembre 2023 pour plus d'information.

### Risque

- Déni de service
- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance

## Annexe

Bulletins de sécurité Cisco du 27 Septembre 2023:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-getvpn-rce-g8qR68sx>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aaascp-Tyj4fEJm>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appqoe-utd-dos-p8O57p5y>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat3k-dos-ZZA4Gb3r>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ins-acc-con-nHAVDRBZ>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-l2tp-dos-eB5tuFmV>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlre-H93FswRz>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdij-FzZAeXAY>