



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans les produits Cisco
<b>Numéro de Référence</b>	43391708/23
<b>Date de Publication</b>	17 Août 2023
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- Cisco Duo Device Health Application (Windows) versions 5.0.0 et 5.1.0 antérieures à 5.2.0
- Cisco Secure Endpoint Connector (Linux) versions antérieures à 1.22.0
- Cisco Secure Endpoint Connector (MacOS) versions antérieures à 1.22.0
- Cisco Secure Endpoint Connector (Windows) versions antérieures à 8.1.7.21585
- Cisco Secure Endpoint Private Cloud versions antérieures à 3.8.0
- Cisco ThousandEyes Enterprise Agent versions antérieures à 0.218
- Cisco Unified CM et Unified CM SME versions 11.5(1) et 12.5(1) antérieures à 12.5(1)SU8
- Cisco Unified CM et Unified CM SME versions 14 sans le correctif de sécurité ciscocm.V14SU3\_CSCwe89928\_sql-injection\_C0194-1.cop.sha512

### Identificateurs externes

- CVE-2023-20197 , CVE-2023-20211 , CVE-2023-20212 , CVE-2023-20224 , CVE-2023-20229

### 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

Veillez se référer au bulletin de sécurité Cisco du 16 août 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 16 août 2023:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thoueye-privesc-NVhHGwb3>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-dha-filewrite-xPMBMZAK>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-injection-g6MbwH2>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-rNwNEEee>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-FTkhqMWZ>