



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Cisco
Numéro de Référence	39872001/23
Date de Publication	20 janvier 2023
Risque	Important
Impact	Important

Systemes affectés

- Cisco Email Security Appliance (ESA)
- Cisco Expressway Series et Cisco TelePresence VCS versions antérieures à 14.0.7
- Cisco Unified Communications Manager versions 11.5.x et 12.5.x antérieures à 12.5(1)SU7
- Cisco Unified Communications Manager versions 14.x antérieures à 14SU3 (correctif prévu pour mars 2023)

Identificateurs externes

- CVE-2023-20010, CVE-2023-20057, CVE-2022-20806,
- CVE-2022-20807, CVE-2022-20809

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 18 janvier 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 18 janvier 2023 :

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-sql-rpPczR8n>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-bsFVwueV>