



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Cisco
Numéro de Référence	43492508/23
Date de Publication	25 Août 2023
Risque	Important
Impact	Important

Systèmes affectés

- UCS versions antérieures à 4.1(3l)
- UCS versions 4.2(x) antérieures à 4.2(3b)
- UCS versions 4.2(x) antérieures à 4.2(3d) pour Cisco UCS 6324 Fabric Interconnects
- Firepower 4100 ,Firepower 9300 Security Appliances
- les commutateurs séries Nexus 3000 et 9000 versions 9.3(11), 10.2(5) et 10.3(2)

Identificateurs externes

- CVE-2023-20200, CVE-2023-20169, CVE-2023-20168

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.

Solution

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

Risque

- Déni de service

Annexe

Bulletins de sécurité Cisco du 01 Février 2023:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp-ucsf-snmp-dos-qtv69NAO>
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-n3_9k-isis-dos-FTCXB4Vb
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-remoteauth-dos-XB6pv74m>