

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 28-02-2023

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans les produits Cisco
Référence	1028
Date de Publication	2023-02-16
Sévérité	Elevé

IMPACT :

- Déni de service
- Exécution de code arbitraire
- Perte de confidentialité
- Perte d'intégrité

SYSTÈME AFFECTÉ :

- Cisco Email Security Appliance versions antérieures à 12.5.4-041, antérieures à 13.0.5-007, antérieures à 13.5.4-038, antérieures à 14.2.1-020, antérieures à 14.3.0-032
- Cisco Secure Email and Web Manager versions antérieures à 12.8.1-021, antérieures à 13.8.1-108, antérieures à 14.2.0-224, antérieures à 14.2.1-020, antérieures à 14.3.0-120
- Cisco Nexus Dashboard version antérieures à 2.3(1c)
- Cisco Secure Endpoint pour Linux versions antérieures à 1.20.2, pour MacOS versions antérieures à 1.21, pour Windows versions antérieures à 7.5.9 et 8.1.5
- Cisco Secure Endpoint Private Cloud versions antérieures à 3.6.0
- Cisco Secure Web Appliance versions antérieures à 14.0.4-005 et 15.0.0-254

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans les systèmes Cisco susmentionné. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance, de porter atteinte à la confidentialité de données, de réussir un deni de service et une perte d'intégrité.

SOLUTION :

Mettre à jour vos Cisco.(se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Cisco Security Advisory 15-02-2023

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndb-dnsdos-bYscZOSu>

- CVE-2023-20009

<https://www.cve.org/CVERecord?id=CVE-2023-20009>

- CVE-2023-20014

<https://www.cve.org/CVERecord?id=CVE-2023-20014>

- CVE-2023-20032

<https://www.cve.org/CVERecord?id=CVE-2023-20032>

- CVE-2023-20075

<https://www.cve.org/CVERecord?id=CVE-2023-20075>