DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 06-07-2024

BULLETIN ALERTES

Object	Vulnérabilité dans les produits Cisco NX-OS
Réference	1181
Date de Publication	2024-07-06
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données

SYSTÉME AFFECTÉ :

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

DÉSCRIPTION :

Une vulnérabilité a été découverte dans les produits Cisco NX-OS. Un attaquant pourrait exploiter cette vulnérabilité en incluant une entrée spécialement conçue comme argument d'une commande CLI de configuration affectée. Une exploitation réussie pourrait permettre à l'attaquant d'exécuter des commandes arbitraires sur le système d'exploitation avec les privilèges de root.

NB : La vulnérabilité (CVE-2024-20399) est activement exploitée.

SOLUTION :

Mettre à jour vos produits Cisco NX-OS. (se référer à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Cisco du 03-07-2024

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP

- CVE-2024-20399
  https://www.cve.org/CVERecord?id=CVE-2024-20399