Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 03 mars 2016
N° CERTFR-2016-AVI-079

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans les commutateurs Cisco Nexus séries 3000 et 3500

Gestion du document

Référence	CERTFR-2016-AVI-079
Titre	Vulnérabilité dans les commutateurs Cisco Nexus séries 3000 et 3500
Date de la première version	03 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160302-n3k du 02 mars 2016
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

– contournement de la politique de sécurité

2 - Systèmes affectés

– Commutateurs Cisco Nexus séries 3000 exécutant Cisco NX-OS versions 6.0(2)U6(x) antérieures à 6.0(2)U6(5a)
– Commutateurs Cisco Nexus séries 3500 exécutant Cisco NX-OS versions 6.0(2)A6(x) antérieures à 6.0(2)A6(5a)
– Commutateurs Cisco Nexus séries 3500 exécutant Cisco NX-OS versions 6.0(2)A7(x) antérieures à 6.0(2)A7(1a)

3 - Résumé

Une vulnérabilité a été corrigée dans *les commutateurs Cisco Nexus séries 3000 et 3500*. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Cisco cisco-sa-20160302-n3k du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-n3k
- Référence CVE CVE-2016-1329
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1329

Gestion détaillée du document

03 mars 2016 version initiale.