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 10 mai 2017
N° CERTFR-2017-ALE-005

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans les commutateurs Cisco

Gestion du document

Référence	CERTFR-2017-ALE-005
Titre	Vulnérabilité dans les commutateurs Cisco
Date de la première version	20 mars 2017
Date de la dernière version	10 mai 2017
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170317-cmp du 17 mars 2017
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)

– exécution de code arbitraire à distance

2 - Systèmes affectés

les commutateurs Cisco exécutant Cisco IOS ou Cisco IOS XE

3 - Résumé

Une vulnérabilité a été découverte dans *les commutateurs Cisco*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Description

Une vulnérabilité dans l'implémentation du Cisco *Cluster Management Protocol* (CMP) permet une exécution de code à distance dans les commutateurs Cisco exécutant Cisco IOS ou Cisco IOS XE.
Se référer au bulletin de l'éditeur pour une liste exhaustive des produits impactés (cf. section Documentation).
Ce protocole utilise le service Telnet afin que les membres d'un groupe puissent dialoguer entre eux.

Cette vulnérabilité est due à deux facteurs.
Le premier est que les communications Telnet sont traitées même si elles proviennent d'en dehors du groupe.

Le deuxième est qu'une session Telnet spécifique à CMP peut provoquer un débordement de tampon.
A noter que le seul fait de commuter une trame comportant une charge malveillante ne suffit pas à déclencher la vulnérabilité, la communication piégée doit être destinée à l'équipement vulnérable.
Cisco n'a pas annoncé de date de sortie d'un correctif de sécurité.

En attendant, le CERT-FR recommande dans un premier temps de suivre les bonnes pratiques en matière de sécurité informatique en s'assurant que l'accès aux interfaces d 'administration des équipements réseaux soit restreint à un canal interne de confiance.
Ensuite, le CERT-FR recommande de privilégier le protocole SSH à Telnet.
Enfin, si désactiver les communications Telnet n'est pas une option viable, Cisco fournit des règles de détection réseau (cf. section Documentation).
A noter que les règles de détection SNORT 41909 et 41910 sont disponibles gratuitement à condition d'avoir créé un compte Snort. Celles-ci sont contenues dans le fichier *server-other.so* et sont de type *TRUFFLEHUNTER*, c'est à dire que leur contenu est dissimulé.

5 - Solution

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

6 - Documentation

- Avis CERT-FR CERTFR-2017-AVI-143
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-143/index.html
- Bulletin de sécurité Cisco cisco-sa-20170317-cmp du 17 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp
- Cisco IOS CMP Buffer Overflow
  https://tools.cisco.com/security/center/viewIpsSignature.x?signatureId=7880&signatureSubId=0&softwareVersion=6.0&relea
- Snort
  https://www.snort.org/downloads
- Référence CVE CVE-2017-3881
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3881

Gestion détaillée du document

20 mars 2017 version initiale.
10 mai 2017 clôture de l'alerte.