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 25 février 2016
N° CERTFR-2016-AVI-071

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-071
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	25 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160224-ace du 24 février 2016 Bulletin de sécurité Cisco cisco-sa-20160224-fmc du 24 février 2016 Bulletin de sécurité Cisco cisco-sa-20160223-nx2000 du 23 février 2016 Bulletin de sécurité Cisco cisco-sa-20160218-glibc du 18 février 2016 Bulletin de sécurité Cisco cisco-sa-20160218-asr du 18 février 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)

- exécution de code arbitraire à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Cisco ACE 4710 Application Control Engine exécutant les versions A5(3.0) et antérieures
- Cisco FirePOWER Management Center versions 5.x et 6.0.0.x
- Cisco Nexus 2000 Series Fabric Extenders
- Cisco ASR 5000 devices exécutant les versions de StarOS antérieures à 19.3.M0.62771 et antérieures à 20.0.M0.62768
- Voir sur le site du constructeur la liste des systèmes affectés par la vulnérabilité CVE-2015-7547 concernant la glibc (lien fourni dans la section Documentation)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

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-20160224-ace du 24 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160224-ace
- Bulletin de sécurité Cisco cisco-sa-20160224-fmc du 24 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160224-fmc
- Bulletin de sécurité Cisco cisco-sa-20160223-nx2000 du 23 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160223-nx2000
- Bulletin de sécurité Cisco cisco-sa-20160218-glibc du 18 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-glibc
- Bulletin de sécurité Cisco cisco-sa-20160218-asr du 18 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-asr
- Référence CVE CVE-2015-7547
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7547
- Référence CVE CVE-2016-1297
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1297
- Référence CVE CVE-2016-1335
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1335
- Référence CVE CVE-2016-1341
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1341
- Référence CVE CVE-2016-1342
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1342

Gestion détaillée du document

25 février 2016 version initiale.