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 11 février 2016
N° CERTFR-2016-AVI-061

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-061
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	11 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160210-asa-ike du 10 février 2016 Bulletin de sécurité Cisco cisco-sa-20160210-sp1 du 10 février 2016 Bulletin de sécurité Cisco cisco-sa-20160210-sp3 du 10 février 2016 Bulletin de sécurité Cisco cisco-sa-20160210-sp2 du 10 février 2016 Bulletin de sécurité Cisco cisco-sa-20160209-pcp du 09 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
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module pour les commutateurs Cisco de la gamme Catalyst 6500 et les routeurs Cisco de la gamme 7600
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco ISA 3000 Industrial Security Appliance
- Cisco Spark version 2015-07-04
- Cisco Spark version 2015-06
- Cisco Prime Collaboration versions 9.0 et 11.0

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 déni de service à distance et 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-20160210-asa-ike du 10 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike
- Bulletin de sécurité Cisco cisco-sa-20160210-sp1 du 10 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-sp1
- Bulletin de sécurité Cisco cisco-sa-20160210-sp3 du 10 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-sp3
- Bulletin de sécurité Cisco cisco-sa-20160210-sp2 du 10 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-sp2
- Bulletin de sécurité Cisco cisco-sa-20160209-pcp du 09 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160209-pcp
- Référence CVE CVE-2016-1287
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1287
- Référence CVE CVE-2016-1322
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1322
- Référence CVE CVE-2016-1324
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1324
- Référence CVE CVE-2016-1323
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1323
- Référence CVE CVE-2016-1320
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1320

Gestion détaillée du document

11 février 2016 version initiale.