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 20 octobre 2016
N° CERTFR-2016-AVI-354

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-354
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	20 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20161019-asa-idfw du 19 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161019-asa-ca du 19 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161019-fpsnort du 19 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161019-cms du 19 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161019-cms1 du 19 octobre 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
- atteinte à la confidentialité des données
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Cisco ASA versions antérieures à 9.1(7.11)
- Cisco ASA versions 9.2(x) antérieures à 9.2(4.17)
- Cisco ASA versions 9.3(x) antérieures à 9.3(3.11)
- Cisco ASA versions 9.4(x) antérieures à 9.4(3.11)
- Cisco ASA versions 9.5(x) antérieures à 9.5(3.1)
- Cisco ASA versions 9.6(x) antérieures à 9.6(2.1)
- Cisco Firepower System versions antérieures à 5.4.1.6
- Cisco Firepower System versions 6.0.x antérieures à 6.0.1
- Cisco Firepower System versions 6.1.x antérieures à 6.1.0

- Cisco Meeting Server versions antérieures à 2.0.4
- Acano Meeting Server versions 1.8.x antérieures à 1.8.17
- Acano Meeting Server versions 1.9.x antérieures à 1.9.5

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 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-20161019-asa-idfw du 19 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-asa-idfw
- Bulletin de sécurité Cisco cisco-sa-20161019-asa-ca du 19 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-asa-ca
- Bulletin de sécurité Cisco cisco-sa-20161019-fpsnort du 19 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-fpsnort
- Bulletin de sécurité Cisco cisco-sa-20161019-cms du 19 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms
- Bulletin de sécurité Cisco cisco-sa-20161019-cms1 du 19 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161019-cms1
- Référence CVE CVE-2016-6432
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6432
- Référence CVE CVE-2016-6431
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6431
- Référence CVE CVE-2016-6439
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6439
- Référence CVE CVE-2016-6444
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6444
- Référence CVE CVE-2016-6446
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6446

Gestion détaillée du document

20 octobre 2016 version initiale.