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 18 août 2016
N° CERTFR-2016-AVI-284

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-284
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	18 août 2016
Date de la dernière version	23 août 2016
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160817-fmc du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-firepower du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-apic du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-aap du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-aap1 du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-aap2 du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-wms1 du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-ucm du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-ise du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-firepowermc du 17 août 2016 Bulletin de sécurité Cisco cisco-sa-20160817-ippdu 17 août 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
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco Firepower Management Center et Cisco ASA 5500-X Series avec les services FirePOWER versions antérieures à 5.3.1.2
- Cisco Firepower Management Center et Cisco ASA 5500-X Series avec les services FirePOWER versions 5.4.0.x antérieures à 5.4.0.1

- Cisco Firepower Management Center et Cisco ASA 5500-X Series avec les services FirePOWER versions 5.4.x antérieures à 5.4.1
- Cisco Firepower Management Center et Cisco ASA 5500-X Series avec les services FirePOWER versions antérieures à 6.0.0
- Cisco Firepower Management Center et Cisco ASA 5500-X Series avec les services FirePOWER versions antérieures à 5.3.0.3
- Cisco APIC-EM versions antérieures à 1.2
- Cisco Aironet 1800, 2800, et 3800 AP platforms versions antérieures à 8.2.110.0, 8.2.121.0 ou 8.3.102.0
- Cisco WebEx Meetings Server version 2.6 sans le dernier correctif de sécurité
- Cisco Unified Communications Manager version 11.5 sans le dernier correctif de sécurité
- Cisco Identity Services Engine version 1.3(0.876) sans le dernier correctif de sécurité
- Cisco Firepower Management Center version 4.10.3 sans le dernier correctif de sécurité
- Cisco Firepower Management Center version 5.2.0 sans le dernier correctif de sécurité
- Cisco Firepower Management Center version 5.3.0 sans le dernier correctif de sécurité
- Cisco Firepower Management Center version 5.3.0.2 sans le dernier correctif de sécurité
- Cisco Firepower Management Center version 5.3.1 sans le dernier correctif de sécurité
- Cisco Firepower Management Center version 5.4.0 sans le dernier correctif de sécurité
- Cisco IP Phone 8800 Series version 11.0(1) sans le dernier correctif de sécurité

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-20160817-fmc du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-fmc
- Bulletin de sécurité Cisco cisco-sa-20160817-firepower du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-firepower
- Bulletin de sécurité Cisco cisco-sa-20160817-apic du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-apic
- Bulletin de sécurité Cisco cisco-sa-20160817-aap2 du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap2
- Bulletin de sécurité Cisco cisco-sa-20160817-aap1 du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap1
- Bulletin de sécurité Cisco cisco-sa-20160817-aap du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-aap
- Bulletin de sécurité Cisco cisco-sa-20160817-wms1 du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-wms1
- Bulletin de sécurité Cisco cisco-sa-20160817-ucm du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ucm
- Bulletin de sécurité Cisco cisco-sa-20160817-ise du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ise
- Bulletin de sécurité Cisco cisco-sa-20160817-firepowermc du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-firepowermc
- Bulletin de sécurité Cisco cisco-sa-20160817-ippdu 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-ipp

- Référence CVE CVE-2016-1365
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1365
- Référence CVE CVE-2016-1457
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1457
- Référence CVE CVE-2016-1458
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1458
- Référence CVE CVE-2016-1479
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1479
- Référence CVE CVE-2016-1484
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1484
- Référence CVE CVE-2016-1485
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1485
- Référence CVE CVE-2016-6361
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6361
- Référence CVE CVE-2016-6362
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6362
- Référence CVE CVE-2016-6363
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6363
- Référence CVE CVE-2016-6364
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6364
- Référence CVE CVE-2016-6365
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6365

Gestion détaillée du document

18 août 2016 version initiale.

23 août 2016 changement 'Cisco APIC-EM version 1.0 sans le dernier correctif de sécurité' à 'Cisco APIC-EM versions antérieures à 1.2' dans systèmes affectés