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 06 mai 2016
N° CERTFR-2016-AVI-153

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-153
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	06 mai 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160504-tpxml du 04 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160504-firepower du 04 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160504-fpkern du 04 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160504-finesse du 04 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160504-openssl du 04 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160503-pca du 03 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160428-cis du 28 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160428-cwms du 28 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160428-apic du 28 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160428-ntpd du 28 avril 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)

- déni de service à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco TelePresence EX Series, Integrator C Series, MX Series, Profile Series, SX Series, SX Quick Set Series, VX Clinical Assistant et VX Tactical exécutant les versions suivantes : TC 7.2.0, TC 7.2.1, TC 7.3.0, TC 7.3.1, TC 7.3.2, TC 7.3.3, TC 7.3.4, TC 7.3.5, CE 8.0.0, CE 8.0.1, ou CE 8.1.0
- Cisco FirePOWER versions 5.3.x antérieures à 5.3.0.7
- Cisco FirePOWER versions 5.4.x antérieures à 5.4.0.4
- Cisco ASA 5585-X FirePOWER SSP versions 5.3.1.x antérieures à 5.3.1.7

- Cisco ASA 5585-X FirePOWER SSP versions 5.4.0.x antérieures à 5.4.0.7
- Cisco ASA 5585-X FirePOWER SSP versions 5.4.1.x antérieures à 5.4.1.6
- Cisco ASA 5585-X FirePOWER SSP versions 6.0.x antérieures à 6.0.1
- Cisco Finesse
- Cisco Prime Collaboration Assurance Software versions 10.5 à 11.0
- Cisco Information Server version 6.2
- Cisco WebEx Meetings Server version 2.6
- Cisco APIC-EM version 1.0(1)
- Voir sur le site du constructeur pour les systèmes affectés par les vulnérabilités du Network Time Protocol Daemon (cf. section Documentation)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer un déni de service 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-20160504-tpxml du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-tpxml
- Bulletin de sécurité Cisco cisco-sa-20160504-firepower du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-firepower
- Bulletin de sécurité Cisco cisco-sa-20160504-fpkern du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-fpkern
- Bulletin de sécurité Cisco cisco-sa-20160504-finesse du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-finesse
- Bulletin de sécurité Cisco cisco-sa-20160504-openssl du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-openssl
- Bulletin de sécurité Cisco cisco-sa-20160503-pca du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160503-pca
- Bulletin de sécurité Cisco cisco-sa-20160428-cis du 04 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-cis
- Bulletin de sécurité Cisco cisco-sa-20160428-cwms du 28 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-cwms
- Bulletin de sécurité Cisco cisco-sa-20160428-apic du 28 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-apic
- Bulletin de sécurité Cisco cisco-sa-20160428-ntpd du 28 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-ntpd
- Référence CVE CVE-2015-7704
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7704
- Référence CVE CVE-2015-8138
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8138
- Référence CVE CVE-2016-1343
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1343
- Référence CVE CVE-2016-1368
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1368
- Référence CVE CVE-2016-1369
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1369

- Référence CVE CVE-2016-1373
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1373
- Référence CVE CVE-2016-1386
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1386
- Référence CVE CVE-2016-1387
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1387
- Référence CVE CVE-2016-1389
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1389
- Référence CVE CVE-2016-1392
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1392
- Référence CVE CVE-2016-1547
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1547
- Référence CVE CVE-2016-1548
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1548
- Référence CVE CVE-2016-1549
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1549
- Référence CVE CVE-2016-1550
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1550
- Référence CVE CVE-2016-1551
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1551
- Référence CVE CVE-2016-2105
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2105
- Référence CVE CVE-2016-2106
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2106
- Référence CVE CVE-2016-2107
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107
- Référence CVE CVE-2016-2108
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2108
- Référence CVE CVE-2016-2109
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2109
- Référence CVE CVE-2016-2176
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2176
- Référence CVE CVE-2016-2516
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2516
- Référence CVE CVE-2016-2517
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2517
- Référence CVE CVE-2016-2518
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2518
- Référence CVE CVE-2016-2519
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2519

Gestion détaillée du document

06 mai 2016 version initiale.