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 03 mars 2016
N° CERTFR-2016-AVI-080

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-080
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	03 mars 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité les produits Cisco cisco-sa-20160302-netstack du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-n5ksnmp du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-wsa du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-openssl du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-psc du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160226-vds-is du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-cpi1 du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-cucdm du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-FireSIGHT du 02 mars 2016 Bulletin de sécurité les produits Cisco cisco-sa-20160302-FireSIGHT1 du 02 mars 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
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- injection de code indirecte à distance

2 - Systèmes affectés

- Commutateurs Cisco Nexus séries 1000V, 3000, 4000, 5000, 6000 et 7000
- Commutateurs Cisco Nexus séries 5500, 5600 et 6000 exécutant les versions de Cisco NX-OS 7.1 antérieures à 7.1(2)N1(1)
- Cisco Web Security Appliance (WSA) exécutant les versions d'AsyncOS antérieures à 8.5.3-051 et 9.0.0-485.

- Voir le site du constructeur pour la liste des systèmes potentiellement affectés par les vulnérabilités concernant OpenSSL (lien fourni dans la section Documentation)
- Cisco Policy Suite versions 7.0.1.3, 7.0.2, 7.0.2-att, 7.0.3-att, 7.0.4-att, et 7.5.0
- Cisco VDS-IS versions 3.3(0), 3.3(1), 4.0(0), et 4.1(0)
- Cisco Prime Infrastructure version 3.0
- Cisco Unified Communications Domain Manager versions 8.x antérieures à 8.1.1
- Cisco FireSIGHT System Software version 6.1.0

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à l'intégrité des données 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 les produits Cisco cisco-sa-20160302-netstack du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-netstack
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-n5ksnmp du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-n5ksnmp
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-wsa du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-wsa
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-openssl du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-openssl
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-psc du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-psc
- Bulletin de sécurité les produits Cisco cisco-sa-20160226-vds-is du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160226-vds-is
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-cpi1 du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cpi1
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-cucdm du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-cucdm
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-FireSIGHT du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-FireSIGHT
- Bulletin de sécurité les produits Cisco cisco-sa-20160302-FireSIGHT1 du 02 mars 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160302-FireSIGHT1
- Référence CVE CVE-2015-0718
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0718
- Référence CVE CVE-2015-6260
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6260
- Référence CVE CVE-2016-0702
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0702
- Référence CVE CVE-2016-0703
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0703
- Référence CVE CVE-2016-0704
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0704
- Référence CVE CVE-2016-0705
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0705
- Référence CVE CVE-2016-0797
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0797

- Référence CVE CVE-2016-0798
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0798
- Référence CVE CVE-2016-0799
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0799
- Référence CVE CVE-2016-0800
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
- Référence CVE CVE-2016-1288
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1288
- Référence CVE CVE-2016-1353
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1353
- Référence CVE CVE-2016-1354
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1354
- Référence CVE CVE-2016-1355
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1355
- Référence CVE CVE-2016-1356
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1356
- Référence CVE CVE-2016-1357
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1357
- Référence CVE CVE-2016-1359
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1359

Gestion détaillée du document

03 mars 2016 version initiale.