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 avril 2017
N° CERTFR-2017-AVI-127

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-127
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	20 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170419-asa-dns du 19 avril 2017 Bulletin de sécurité Cisco cisco-sa-20170419-asa-ipsec du 19 avril 2017 Bulletin de sécurité Cisco cisco-sa-20170419-asa-tls du 19 avril 2017 Bulletin de sécurité Cisco cisco-sa-20170419-asa-xauth du 19 avril 2017 Bulletin de sécurité Cisco cisco-sa-20170419-energywise du 19 avril 2017 Bulletin de sécurité Cisco cisco-sa-20170419-fpsnort du 19 avril 2017 Bulletin de sécurité Cisco cisco-sa-20170419-ucm du 19 avril 2017
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

2 - Systèmes affectés

- Cisco ASA 1000V Cloud Firewall (voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)
- Cisco ASA 5500 Series Adaptive Security Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)
- Cisco ASA 5500-X Series Next-Generation Firewalls (voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)
- Cisco ASA Services Module pour les commutateurs Cisco Catalyst séries 6500 et les routeurs Cisco séries 7600 (voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)
- Cisco Adaptive Security Virtual Appliance (ASAv, voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)

- Cisco Firepower 9300 ASA Security Module (voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)
- Cisco ISA 3000 Industrial Security Appliance (voir sur le site du constructeur pour les versions vulnérables de Cisco ASA)
- Adaptive Security Appliance (ASA) 5500-X Series with FirePOWER Services (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Advanced Malware Protection (AMP) for Networks, 7000 Series Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Firepower 4100 Series Security Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- FirePOWER 7000 Series Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- FirePOWER 8000 Series Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Firepower 9300 Series Security Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- FirePOWER Threat Defense for Integrated Services Routers (ISRs, voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Industrial Security Appliance 3000 (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Sourcefire 3D System Appliances (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware (voir sur le site du constructeur pour les versions vulnérables de Cisco Firepower System)
- Cisco Unified Communications Manager (CallManager) sans le dernier correctif de sécurité
- Cisco IOS et Cisco IOS XE avec le module EnergyWise activé, sans le dernier correctif de sécurité

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.

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-20170419-asa-dns du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns
- Bulletin de sécurité Cisco cisco-sa-20170419-asa-ipsec du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-ipsec
- Bulletin de sécurité Cisco cisco-sa-20170419-asa-tls du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-tls
- Bulletin de sécurité Cisco cisco-sa-20170419-asa-xauth du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-xauth
- Bulletin de sécurité Cisco cisco-sa-20170419-energywise du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-energywise

- Bulletin de sécurité Cisco cisco-sa-20170419-fpsnort du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-fpsnort
- Bulletin de sécurité Cisco cisco-sa-20170419-ucm du 19 avril 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-ucm
- Référence CVE CVE-2016-6368
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6368
- Référence CVE CVE-2017-3808
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3808
- Référence CVE CVE-2017-3860
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3860
- Référence CVE CVE-2017-3861
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3861
- Référence CVE CVE-2017-3862
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3862
- Référence CVE CVE-2017-3863
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3863
- Référence CVE CVE-2017-6607
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6607
- Référence CVE CVE-2017-6608
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6608
- Référence CVE CVE-2017-6609
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6609
- Référence CVE CVE-2017-6610
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6610

Gestion détaillée du document

20 avril 2017 version initiale.