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 5 septembre 2016
N° CERTFR-2016-ALE-005

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Multiples vulnérabilités dans les pare-feux Cisco

Gestion du document

Référence	CERTFR-2016-ALE-005
Titre	Multiples vulnérabilités dans les pare-feux Cisco
Date de la première version	18 août 2016
Date de la dernière version	5 septembre 2016
Source(s)	Bulletin de sécurité cisco-sa-20160817-asa-snmp Cisco du 17 août 2016 Bulletin de sécurité cisco-sa-20160817-asa-cli Cisco du 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

2 - Systèmes affectés

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module pour Cisco Catalyst 6500 Series Switches et Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco PIX Firewalls
- Cisco Firewall Services Module (FWSM)
- Cisco Firepower 4100 Series
- Cisco Firepower Threat Defense Software
- Cisco Industrial Security Appliance 3000

3 - Résumé

De multiples vulnérabilités ont été découvertes dans *les pare-feux Cisco*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Description

Le samedi 13 août, des attaquants se faisant appeler les Shadow Brokers ont publiquement révélé des outils offensifs, qu'ils affirment provenir d'Equation, un groupe d'élite lié à la NSA.
Parmi ces outils se trouve du code malveillant dont la fonction est d'exploiter des vulnérabilités dans les pare-feux Cisco afin d'en prendre le contrôle.
Dans ses bulletins de sécurité cisco-sa-20160817-asa-snmp et cisco-sa-20160817-asa-cli (cf. Section Documentation), l'équipementier énumère la liste de produits pour lesquels un correctif est disponible.
Le CERT-FR recommande de durcir ses équipements tout en respectant les bonnes pratiques (cf. Section Documentation).
Des règles de détection réseau sont également disponibles, soit de manière payante (Cisco, cf. Section Documentation), soit à titre gratuit (Emerging Threats, cf. Section Documentation).

5 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation)

6 - Documentation

- Avis CERTFR-2016-AVI-295
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-295
- Bulletin de sécurité cisco-sa-20160817-asa-snmp Cisco du 17 août 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp
- Bulletin de sécurité cisco-sa-20160817-asa-cli Cisco du 17 août 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli
- Blog Cisco : The Shadow Brokers
  http://blogs.cisco.com/security/shadow-brokers
- Guide de durcissement des pare-feux Cisco ASA
  http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/200150-Cisco-Guide-to-Harden-Cisco-ASA-Firewall.html
- Guide de durcissement des équipements Cisco
  https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- Guide de vérification d'intégrité ASA
  http://www.cisco.com/c/en/us/about/security-center/intelligence/asa-integrity-assurance.html
- Blog Cisco : Analyse de l'intégrité d'une image IOS
  https://blogs.cisco.com/security/offline-analysis-of-ios-image-integrity
- Règle de détection réseau Emerging Threats 1
  http://docs.emergingthreats.net/bin/view/Main/2023070
- Règle de détection réseau Emerging Threats 2
  http://doc.emergingthreats.net/bin/view/Main/2023071
- Change logs des règles Snort soumises à abonnement
  https://www.snort.org/advisories/talos-rules-2016-08-16
- Annonce de fin de vie des Cisco Firewall Services Modules (FWSM)
  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-series-firewall-services-module/eol$_c$51 $-$ 699134.$html$
- Annonce de fin de vie des Cisco PIX Firewalls
  http://www.cisco.com/c/en/us/products/security/pix-500-series-security-appliances/eos-eol-notice-listing.html
- Référence CVE CVE-2016-6366
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6366
- Référence CVE CVE-2016-6367
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6367

Gestion détaillée du document

18 août 2016 version initiale.

23 août 2016 ajout de produits sur la liste des systèmes affectés ainsi que les annonces de fin de vie des produits Cisco Firewall Services Module et Cisco PIX Firewalls.

5 septembre 2016 clôture de l'alerte.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2016-ALE-005`