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 27 octobre 2016
N° CERTFR-2016-AVI-363

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-363
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	27 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20161026-ipics du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esa2 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esa1 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esa3 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esa5 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esa6 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esawsa1 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esawsa2 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-esawsa3 du 26 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161026-ipics2 du 26 octobre 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
- élévation de privilèges

2 - Systèmes affectés

- Cisco IPICS versions antérieures à 4.10(2)
- Cisco AsyncOS toutes versions sans le dernier correctif de sécurité
- Cisco Email Security Appliance (ESA) 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, un contournement de la politique de sécurité et une élévation de privilèges.

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 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-ipics
- Bulletin de sécurité Cisco cisco-sa-20161026-esa2 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa2
- Bulletin de sécurité Cisco cisco-sa-20161026-esa1 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa1
- Bulletin de sécurité Cisco cisco-sa-20161026-esa3 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa3
- Bulletin de sécurité Cisco cisco-sa-20161026-esa5 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa5
- Bulletin de sécurité Cisco cisco-sa-20161026-esa6 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esa6
- Bulletin de sécurité Cisco cisco-sa-20161026-esawsa1 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esawsa1
- Bulletin de sécurité Cisco cisco-sa-20161026-esawsa2 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esawsa2
- Bulletin de sécurité Cisco cisco-sa-20161026-esawsa3 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-esawsa3
- Bulletin de sécurité Cisco cisco-sa-20161026-ipics2 du 26 octobre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161026-ipics2
- Référence CVE CVE-2016-1480
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1480
- Référence CVE CVE-2016-1481
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1481
- Référence CVE CVE-2016-1486
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1486
- Référence CVE CVE-2016-6356
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6356
- Référence CVE CVE-2016-6357
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6357
- Référence CVE CVE-2016-6358
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6358
- Référence CVE CVE-2016-6360
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6360
- Référence CVE CVE-2016-6372
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6372
- Référence CVE CVE-2016-6397
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6397
- Référence CVE CVE-2016-6430
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6430

Gestion détaillée du document

27 octobre 2016 version initiale.

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-AVI-363