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 19 mai 2016
N° CERTFR-2016-AVI-177

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-177
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	19 mai 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160518-wsa1 du 18 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160518-wsa2 du 18 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160518-wsa3 du 18 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160518-wsa4 du 18 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160517-ise du 17 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160517-ucs du 17 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160517-asa-xml du 17 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160517-asa-vpn du 17 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160516-vcs du 16 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160513-ies du 13 mai 2016 Bulletin de sécurité Cisco cisco-sa-20160510-cnap du 10 mai 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
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco AsyncOS versions antérieures à 9.0.1-162 pour Cisco WSA
- Cisco Identity Services Engine (ISE) versions antérieures à 1.2.0.899 patch 7
- Cisco Unified Computing System (UCS) Central Software version 1.4(1a)
- Cisco ASA versions antérieures à 9.1(7.6)
- Cisco ASA versions 9.2x antérieures à 9.2(4.8)

- Cisco ASA versions 9.3x antérieures à 9.3(3.8)
- Cisco ASA versions 9.4x antérieures à 9.4(2.6)
- Cisco ASA versions 9.5x antérieures à 9.5(2.6)
- Cisco TelePresence VCS X8.x versions antérieures à X8.7.2
- Commutateurs Cisco Industrial Ethernet séries 4000 exécutant Cisco IOS versions antérieures à 15.2(2)EA3 et 15.2(4)EA1
- Commutateurs Cisco Industrial Ethernet séries 5000 exécutant Cisco IOS versions antérieures à 15.2(2)EB2
- Cisco Cloud Network Automation Provisioner versions 1.0 et 1.1

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 injection de code indirecte à distance (XSS).

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-20160518-wsa1 du 18 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa1
- Bulletin de sécurité les produits Cisco cisco-sa-20160518-wsa2 du 18 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa2
- Bulletin de sécurité les produits Cisco cisco-sa-20160518-wsa3 du 18 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa3
- Bulletin de sécurité les produits Cisco cisco-sa-20160518-wsa4 du 18 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa4
- Bulletin de sécurité les produits Cisco cisco-sa-20160517-ise du 17 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-ise
- Bulletin de sécurité les produits Cisco cisco-sa-20160517-ucs du 17 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-ucs
- Bulletin de sécurité les produits Cisco cisco-sa-20160517-asa-xml du 17 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-asa-xml
- Bulletin de sécurité les produits Cisco cisco-sa-20160517-asa-vpn du 17 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160517-asa-vpn
- Bulletin de sécurité les produits Cisco cisco-sa-20160516-vcs du 16 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160516-vcs
- Bulletin de sécurité les produits Cisco cisco-sa-20160513-ies du 13 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160513-ies
- Bulletin de sécurité les produits Cisco cisco-sa-20160510-cnap du 10 mai 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160510-cnap
- Référence CVE CVE-2016-1379
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1379
- Référence CVE CVE-2016-1380
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1380
- Référence CVE CVE-2016-1381
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1381
- Référence CVE CVE-2016-1382
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1382
- Référence CVE CVE-2016-1383
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1383

- Référence CVE CVE-2016-1385
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1385
- Référence CVE CVE-2016-1393
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1393
- Référence CVE CVE-2016-1399
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1399
- Référence CVE CVE-2016-1400
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1400
- Référence CVE CVE-2016-1401
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1401
- Référence CVE CVE-2016-1402
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1402

Gestion détaillée du document

19 mai 2016 version initiale.