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 09 novembre 2015
N° CERTFR-2015-AVI-465

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Cisco AsyncOS

Gestion du document

Référence	CERTFR-2015-AVI-465
Titre	Multiples vulnérabilités dans Cisco AsyncOS
Date de la première version	09 novembre 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20151104-esa2 du 04 novembre 2015 Bulletin de sécurité Cisco cisco-sa-20151104-wsa du 04 novembre 2015 Bulletin de sécurité Cisco cisco-sa-20151104-wsa1 du 04 novembre 2015 Bulletin de sécurité Cisco cisco-sa-20151104-mse-cred du 04 novembre 2015 Bulletin de sécurité Cisco cisco-sa-20151104-aos du 04 novembre 2015 Bulletin de sécurité Cisco cisco-sa-20151104-wsa2 du 04 novembre 2015 Bulletin de sécurité Cisco cisco-sa-20151104-privmse du 04 novembre 2015
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 MSE version 8.0.120.7 et antérieures
- Cisco SMA versions 9.5 et antérieures
- Cisco ESA versions 9.6 et antérieures
- Cisco WSA versions 8.8 et antérieures

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Cisco AsyncOS*. 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 cisco-sa-20151104-esa2 du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-esa2
- Bulletin de sécurité Cisco cisco-sa-20151104-wsa du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-wsa
- Bulletin de sécurité Cisco cisco-sa-20151104-wsa1 du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-wsa1
- Bulletin de sécurité Cisco cisco-sa-20151104-mse-cred du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-mse-cred
- Bulletin de sécurité Cisco cisco-sa-20151104-aos du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-aos
- Bulletin de sécurité Cisco cisco-sa-20151104-wsa2 du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-wsa2
- Bulletin de sécurité Cisco cisco-sa-20151104-privmse du 04 novembre 2015
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151104-privmse
- Référence CVE CVE-2015-6291
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6291
- Référence CVE CVE-2015-6298
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6298
- Référence CVE CVE-2015-6292
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6292
- Référence CVE CVE-2015-6321
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6321
- Référence CVE CVE-2015-6293
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6293
- Référence CVE CVE-2015-4282
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4282
- Référence CVE CVE-2015-6316
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6316

Gestion détaillée du document

09 novembre 2015 version initiale.