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 28 janvier 2016
N° CERTFR-2016-AVI-040

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-040
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	28 janvier 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160127-rv220 du 27 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160127-waascifs du 27 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160127-sbms du 27 janvier 2016 Bulletin de sécurité Cisco cisco-sa-20160127-uc du 27 janvier 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 RV220W Wireless Network Security Firewall versions antérieures à 1.0.7.2
- Cisco Wide Area Application Services Software (WAAS) versions ultérieures à 5.1.1d et antérieures à 5.3.5d
- Cisco Wide Area Application Services Software (WAAS) versions 5.4.x et 5.5.X antérieures à 5.5.3
- Cisco Small Business SG300 Managed Switch version 1.4.1.x
- Cisco Unity Connection version 10.5(2.3009)

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 Cisco cisco-sa-20160127-rv220 du 27 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-rv220
- Bulletin de sécurité Cisco cisco-sa-20160127-waascifs du 27 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-waascifs
- Bulletin de sécurité Cisco cisco-sa-20160127-sbms du 27 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-sbms
- Bulletin de sécurité Cisco cisco-sa-20160127-uc du 27 janvier 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160127-uc
- Référence CVE CVE-2015-6319
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6319
- Référence CVE CVE-2015-6421
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6421
- Référence CVE CVE-2016-1299
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1299
- Référence CVE CVE-2016-1300
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1300

Gestion détaillée du document

28 janvier 2016 version initiale.