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 15 juillet 2016
N° CERTFR-2016-AVI-235

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-235
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	15 juillet 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160713-ncs6k du 13 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160713-asr du 13 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160714-ios-xr du 14 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160714-ms du 14 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160714-wms3 du 14 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160714-wms1 du 14 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160714-wms du 14 juillet 2016 Bulletin de sécurité Cisco cisco-sa-20160714-wms4 du 14 juillet 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
- exécution de code arbitraire
- déni de service à distance
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco IOS XR pour Cisco Network Convergence System 6000
- Cisco ASR 5000 Series versions antérieures à 19.4
- Cisco ASR 5000 Series versions antérieures à 20.1
- Cisco IOS XR Software Release 6.0.1.BASE

- isco Meeting Server Software versions 1.7 à 1.9
- Cisco WebEx Meetings Server version 2.6

3 - Résumé

De multiples vulnérabilités ont été corrigées dans les produits *Cisco*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une exécution de code arbitraire et un déni de service à distance.

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-20160713-ncs6k du 13 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160713-ncs6k
- Bulletin de sécurité Cisco cisco-sa-20160713-asr du 13 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160713-ncs6k
- Bulletin de sécurité Cisco cisco-sa-20160714-ios-xr du 14 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-ios-xr
- Bulletin de sécurité Cisco cisco-sa-20160714-ms du 14 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-ms
- Bulletin de sécurité Cisco cisco-sa-20160714-wms3 du 14 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms3
- Bulletin de sécurité Cisco cisco-sa-20160714-wms1 du 14 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms1
- Bulletin de sécurité Cisco cisco-sa-20160714-wms du 14 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms
- Bulletin de sécurité Cisco cisco-sa-20160714-wms4 du 14 juillet 2016
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160714-wms4
- Référence CVE CVE-2016-1426
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1426
- Référence CVE CVE-2016-1452
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1452
- Référence CVE CVE-2016-1456
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1456
- Référence CVE CVE-2016-1451
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1451
- Référence CVE CVE-2016-1449
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1449
- Référence CVE CVE-2016-1447
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1447
- Référence CVE CVE-2016-1446
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1446
- Référence CVE CVE-2016-1450
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1450

Gestion détaillée du document

15 juillet 2016 version initiale.