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 07 avril 2016
N° CERTFR-2016-AVI-115

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-115
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	07 avril 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160406-remcode du 06 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160406-ucs du 06 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160406-cts2 du 06 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160406-cts du 06 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160406-cts1 du 06 avril 2016 Bulletin de sécurité Cisco cisco-sa-20160406-privauth du 06 avril 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
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Cisco Prime Infrastructure versions antérieures à 3.0.3
- Cisco Evolved Programmable Network Manager (EPNM) versions antérieures à 1.2 MP2 Patch 1
- Cisco Evolved Programmable Network Manager (EPNM) versions antérieures à 1.2 MP4 Patch 2
- Cisco Whiptail Racerunner
- Cisco UCS Invicta Scaling System and Appliance versions antérieures à 5.0.1.3b
- UCS Invicta C3124SA Appliance versions antérieures à 5.0.1.2c
- Cisco TelePresence Server 7010 versions antérieures à 4.2(4.23)

- Cisco TelePresence Server Mobility Services Engine (MSE) 8710 versions antérieures à 4.2(4.23)
- Cisco TelePresence Server on Multiparty Media 310 versions antérieures à 4.2(4.23)
- Cisco TelePresence Server on Multiparty Media 320 versions antérieures à 4.2(4.23)
- Cisco TelePresence Server on Virtual Machine (VM) versions antérieures à 4.2(4.23)

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, un déni de service à distance et un contournement de la politique de sécurité.

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-20160406-remcode du 06 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-remcode
- Bulletin de sécurité Cisco cisco-sa-20160406-ucs du 06 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-ucs
- Bulletin de sécurité Cisco cisco-sa-20160406-cts2 du 06 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-cts2
- Bulletin de sécurité Cisco cisco-sa-20160406-cts du 06 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-cts
- Bulletin de sécurité Cisco cisco-sa-20160406-cts1 du 06 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-cts1
- Bulletin de sécurité Cisco cisco-sa-20160406-privauth du 06 avril 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160406-privauth
- Référence CVE CVE-2016-1291
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1291
- Référence CVE CVE-2016-1313
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1313
- Référence CVE CVE-2015-6312
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6312
- Référence CVE CVE-2016-1346
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1346
- Référence CVE CVE-2015-6313
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6313
- Référence CVE CVE-2016-1290
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1290

Gestion détaillée du document

07 avril 2016 version initiale.