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 12 octobre 2016
N° CERTFR-2016-AVI-343

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-343
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	12 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20161012-waas du 12 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161012-ucm du 12 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161012-prime du 12 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161012-msc du 12 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161012-fin du 12 octobre 2016 Bulletin de sécurité Cisco cisco-sa-20161012-cbr-8 du 12 octobre 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
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- élévation de privilèges
- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

2 - Systèmes affectés

- Cisco Wide Area Application Services (WAAS)
- Cisco Unified Communications Manager (CUCM)
- Cisco Prime Infrastructure
- Cisco Evolved Programmable Network Manager
- Cisco Meeting Server versions antérieures à 2.0.6 avec XMPP activé
- Acano Server versions antérieures à 1.8.18 et 1.9.6 avec XMPP activé
- Cisco Finesse

– Cisco cBR-8 Converged Broadband Routers versions 3.17S, 3.17S, 3.18.0S, 3.18.1S, 3.18.0SP

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 atteinte à l'intégrité des données et une atteinte à la confidentialité des données.

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-20161012-waas du 12 octobre 2016
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-waas
– Bulletin de sécurité Cisco cisco-sa-20161012-ucm du 12 octobre 2016
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-ucm
– Bulletin de sécurité Cisco cisco-sa-20161012-prime du 12 octobre 2016
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-prime
– Bulletin de sécurité Cisco cisco-sa-20161012-msc du 12 octobre 2016
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-msc
– Bulletin de sécurité Cisco cisco-sa-20161012-fin du 12 octobre 2016
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-fin
– Bulletin de sécurité Cisco cisco-sa-20161012-cbr-8 du 12 octobre 2016
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161012-cbr-8
– Référence CVE CVE-2016-6438
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6438
– Référence CVE CVE-2016-6442
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6442
– Référence CVE CVE-2016-6445
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6445
– Référence CVE CVE-2016-6443
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6443
– Référence CVE CVE-2016-6440
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6440
– Référence CVE CVE-2016-6437
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6437

Gestion détaillée du document

12 octobre 2016 version initiale.