

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans Cisco APIC-EM

Gestion du document

Référence	CERTFR-2016-AVI-035
Titre	Vulnérabilité dans Cisco APIC-EM
Date de la première version	26 janvier 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160125 du 25 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)

– injection de code indirecte à distance

2 - Systèmes affectés

Cisco APIC-EM version 1.0.10

3 - Résumé

Une vulnérabilité a été corrigée dans *Cisco APIC-EM*. Elle permet à un attaquant de provoquer 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-20160125 du 25 janvier 2016
<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160125-api>

– Référence CVE CVE-2015-6337
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6337>

Gestion détaillée du document

26 janvier 2016 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-035>
