

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-269
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	17 août 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170816-em du 16 août 2017 Bulletin de sécurité Cisco cisco-sa-20170816-apic1 du 16 août 2017 Bulletin de sécurité Cisco cisco-sa-20170816-apic2 du 16 août 2017
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
- élévation de privilèges

2 - Systèmes affectés

- Cisco VNF Element Manager versions antérieures à 5.0.4 et 5.1.4.
- Cisco APIC sans le dernier correctif de sécurité

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges.

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-20170816-em du 16 août 2017
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-em>
- Bulletin de sécurité Cisco cisco-sa-20170816-apic1 du 16 août 2017
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic1>
- Bulletin de sécurité Cisco cisco-sa-20170816-apic2 du 16 août 2017
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170816-apic2>
- Référence CVE CVE-2017-6767
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6767>
- Référence CVE CVE-2017-6768
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6768>
- Référence CVE CVE-2017-6710
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6710>

Gestion détaillée du document

17 août 2017 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-2017-AVI-269>
