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 17 février 2016
N° CERTFR-2016-AVI-065

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2016-AVI-065
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	17 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160216-grid du 16 février 2016 Bulletin de sécurité Cisco cisco-sa-20160216-wap du 16 février 2016 Bulletin de sécurité Cisco cisco-sa-20160215-ie2000 du 15 février 2016 Bulletin de sécurité Cisco cisco-sa-20160215-er du 15 février 2016 Bulletin de sécurité Cisco cisco-sa-20160212-usc du 12 février 2016 Bulletin de sécurité Cisco cisco-sa-20160211-esaamp du 11 février 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)

- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données
- injection de code indirecte à distance

2 - Systèmes affectés

- Cisco 1000 Series Connected Grid Router si la fonctionnalité SNMP est configurée
- Cisco Small Business 500 Series Wireless Access Point version 1.0.4.4
- Cisco Industrial Ethernet 2000 Series Switches exécutant Cisco IOS version 15.2(4)E
- Cisco Emergency Responder version 11.5(0.99833.5)
- Cisco Universal Small Cell devices
- Cisco AMP exécutant Cisco ESA versions 9.5.0-201, 9.6.0-051, et 9.7.0-125

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Cisco*. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité 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-20160216-grid du 16 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160216-grid
- Bulletin de sécurité Cisco cisco-sa-20160216-wap du 16 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160216-wap
- Bulletin de sécurité Cisco cisco-sa-20160215-ie2000 du 15 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160215-ie2000
- Bulletin de sécurité Cisco cisco-sa-20160215-er du 15 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160215-er
- Bulletin de sécurité Cisco cisco-sa-20160212-usc du 12 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160212-usc
- Bulletin de sécurité Cisco cisco-sa-20160211-esaamp du 11 février 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160211-esaamp
- Référence CVE CVE-2016-1333
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1333
- Référence CVE CVE-2016-1334
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1334
- Référence CVE CVE-2016-1330
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1330
- Référence CVE CVE-2016-1331
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1331
- Référence CVE CVE-2016-1321
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1321
- Référence CVE CVE-2016-1315
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1315

Gestion détaillée du document

17 février 2016 version initiale.