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 23 mars 2017
N° CERTFR-2017-AVI-089

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-089
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	23 mars 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170322-iox du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-xeci du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-caf1 du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-caf2 du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-dhcpc du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-l2tp du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-webui du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170322-ztp du 22 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170320-ani du 20 mars 2017 Bulletin de sécurité Cisco cisco-sa-20170320-aniipv6 du 20 mars 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
- déni de service à distance
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco IR809 exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco IR829 exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco IOS XE version 16.2.1 avec le serveur HTTP activé
- Cisco ISR4321 exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco ISR4331 exécutant Cisco IOx versions antérieures à 1.2.4.2

- Cisco ISR4351 exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco ISR4451 exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco ASR1001X exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco ASR1001HX exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco ASR1002X exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco ASR1002HX exécutant Cisco IOx versions antérieures à 1.2.4.2
- Cisco IOS et IOS XE sans le dernier correctif de sécurité

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 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-20170322-iox du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-iox
- Bulletin de sécurité Cisco cisco-sa-20170322-xeci du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-xeci
- Bulletin de sécurité Cisco cisco-sa-20170322-caf1 du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-caf1
- Bulletin de sécurité Cisco cisco-sa-20170322-caf2 du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-caf2
- Bulletin de sécurité Cisco cisco-sa-20170322-dhcpc du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-dhcpc
- Bulletin de sécurité Cisco cisco-sa-20170322-l2tp du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-l2tp
- Bulletin de sécurité Cisco cisco-sa-20170322-webui du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-webui
- Bulletin de sécurité Cisco cisco-sa-20170322-ztp du 22 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170322-ztp
- Bulletin de sécurité Cisco cisco-sa-20170320-ani du 20 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-ani
- Bulletin de sécurité Cisco cisco-sa-20170320-aniipv6 du 20 mars 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170320-aniipv6
- Référence CVE CVE-2017-3853
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3853
- Référence CVE CVE-2017-3858
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3858
- Référence CVE CVE-2017-3851
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3851
- Référence CVE CVE-2017-3852
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3852
- Référence CVE CVE-2017-3864
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3864
- Référence CVE CVE-2017-3857
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3857
- Référence CVE CVE-2017-3856
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3856

- Référence CVE CVE-2017-3859
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3859
- Référence CVE CVE-2017-3849
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3849
- Référence CVE CVE-2017-3850
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3850

Gestion détaillée du document

23 mars 2017 version initiale.