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 25 septembre 2014
N° CERTFR-2014-AVI-398

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2014-AVI-398
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	25 septembre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20140924-rsvp du 24 septembre 2014 Bulletin de sécurité Cisco cisco-sa-20140924-mdns du 24 septembre 2014 Bulletin de sécurité Cisco cisco-sa-20140924-metadata du 24 septembre 2014 Bulletin de sécurité Cisco cisco-sa-20140924-sip du 24 septembre 2014 Bulletin de sécurité Cisco cisco-sa-20140924-nat du 24 septembre 2014 Bulletin de sécurité Cisco cisco-sa-20140924-dhcpv6 du 24 septembre 2014
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

2 - Systèmes affectés

De multiples produits sont impactés. Se référer au bulletin de l'éditeur pour la liste exhaustive des produits.

3 - Résumé

De multiples vulnérabilités ont été corrigées dans les produits *Cisco*. Elles permettent à un attaquant de provoquer un déni de service à distance.

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-20140924-rsvp du 24 septembre 2014
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-rsvp
- Bulletin de sécurité Cisco cisco-sa-20140924-mdns du 24 septembre 2014
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-mdns
- Bulletin de sécurité Cisco cisco-sa-20140924-metadata du 24 septembre 2014
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-metadata
- Bulletin de sécurité Cisco cisco-sa-20140924-sip du 24 septembre 2014
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-sip
- Bulletin de sécurité Cisco cisco-sa-20140924-nat du 24 septembre 2014
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-nat
- Bulletin de sécurité Cisco cisco-sa-20140924-dhcpv6 du 24 septembre 2014
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-dhcpv6
- Référence CVE CVE-2014-3354
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3354
- Référence CVE CVE-2014-3358
  http://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2014-3358
- Référence CVE CVE-2014-3356
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3356
- Référence CVE CVE-2014-3355
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3355
- Référence CVE CVE-2014-3360
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3360
- Référence CVE CVE-2014-3361
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3361
- Référence CVE CVE-2014-3359
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3359

Gestion détaillée du document

25 septembre 2014 version initiale.