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 06 juillet 2017
N° CERTFR-2017-AVI-202

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Cisco

Gestion du document

Référence	CERTFR-2017-AVI-202
Titre	Multiples vulnérabilités dans les produits Cisco
Date de la première version	06 juillet 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170705-usf1 du 05 juillet 2017 Bulletin de sécurité Cisco cisco-sa-20170705-usf2 du 05 juillet 2017 Bulletin de sécurité Cisco cisco-sa-20170705-usf3 du 05 juillet 2017 Bulletin de sécurité Cisco cisco-sa-20170705-uas du 05 juillet 2017 Bulletin de sécurité Cisco cisco-sa-20170705-esc1 du 05 juillet 2017 Bulletin de sécurité Cisco cisco-sa-20170705-esc2 du 05 juillet 2017 Bulletin de sécurité Cisco cisco-sa-20170705-asrcmd du 05 juillet 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
- exécution de code arbitraire
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Cisco Ultra Services Framework Staging Server versions antérieures à 5.0.3 et 5.1
- Cisco Ultra Services Framework versions antérieures à 5.0.3 et 5.1
- Cisco Ultra Services Framework UAS versions antérieures à 5.0.3 et 5.1
- Cisco Elastic Services Controller versions antérieures à 2.3.1.434 et 2.3.2
- Cisco StarOS pour ASR 5000 Series, ASR 5500 Series, ASR 5700 Series
- Cisco StarOS pour le logiciel Virtualized Packet Core-Distributed Instance (VPC-DI)

– Cisco StarOS pour le logiciel Virtualized Packet Core-Single Instance (VPC-SI)

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, une exécution de code arbitraire et un contournement de la politique de sécurité.

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-20170705-usf3 du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf3
- Bulletin de sécurité Cisco cisco-sa-20170705-usf1 du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf1
- Bulletin de sécurité Cisco cisco-sa-20170705-uas du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-uas
- Bulletin de sécurité Cisco cisco-sa-20170705-esc2 du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-esc2
- Bulletin de sécurité Cisco cisco-sa-20170705-esc1 du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-esc2
- Bulletin de sécurité Cisco cisco-sa-20170705-usf2 du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf2
- Bulletin de sécurité Cisco cisco-sa-20170705-asrcmd du 05 juillet 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-asrcmd
- Référence CVE CVE-2017-6707
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6707
- Référence CVE CVE-2017-6708
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6708
- Référence CVE CVE-2017-6709
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6709
- Référence CVE CVE-2017-6711
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6711
- Référence CVE CVE-2017-6712
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6712
- Référence CVE CVE-2017-6713
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6713
- Référence CVE CVE-2017-6714
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6714

Gestion détaillée du document

06 juillet 2017 version initiale.