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 19 septembre 2016
N° CERTFR-2016-ALE-007

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Cisco IOS, IOS XE et IOS XR

Gestion du document

Référence	CERTFR-2016-ALE-007
Titre	Vulnérabilité dans Cisco IOS, IOS XE et IOS XR
Date de la première version	19 septembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20160916-ikev1 du 16 septembre 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)

- atteinte à la confidentialité des données

2 - Systèmes affectés

- Cisco IOS XR versions 4.3.x
- Cisco IOS XR versions 5.0.x
- Cisco IOS XR versions 5.1.x
- Cisco IOS XR versions 5.2.x
- Cisco IOS XE toutes versions
- Cisco IOS, voir sur le site du constructeur pour vérifier si votre système est vulnérable (cf. section Documentation)

3 - Résumé

Une vulnérabilité a été découverte dans *Cisco IOS*, *Cisco IOS XE* et *Cisco IOS XR*. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données.

4 - Contournement provisoire

Suite à la fuite de codes d'attaque attribués au groupe Equation le mois dernier, Cisco a enquêté pour déterminer si d'autres de ses produits sont vulnérables à des attaques similaires.
Il s'avère que plusieurs produits peuvent être exploités par une méthode semblable à BENIGNCERTAIN, qui permet à un attaquant d'accéder à des portions de mémoire, dans l'espoir de découvrir des secrets (clés privées, mots de passe...)
Ici, une vulnérabilité dans le code de traitement des paquets IKEv1 de Cisco IOS, IOS XE et IOS XR permet à un attaquant non authentifié de récupérer des portions de mémoire, et ce à distance.
Cisco indique qu'il n'existe pour l'instant pas de mitigations et que cette vulnérabilité est activement exploitée chez certains de ses clients.
Cisco fourni des règles de détection, cependant celles-ci sont soumises à abonnement.
Le CERT-FR recommande l'application des correctifs de sécurité dans les cas où ceux-ci sont disponibles. Sinon, les tunnels IPsec établis sur des systèmes affectés doivent être considérés comme non sécurisés.

5 - Documentation

- Bulletin de sécurité Cisco cisco-sa-20160916-ikev1 du 16 septembre 2016
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1
- Référence CVE CVE-2016-6415
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6415

Gestion détaillée du document

19 septembre 2016 version initiale.