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 31 janvier 2017
N° CERTFR-2017-ALE-001

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Cisco WebEx

Gestion du document

Référence	CERTFR-2017-ALE-001
Titre	Vulnérabilité dans Cisco WebEx
Date de la première version	25 janvier 2017
Date de la dernière version	31 janvier 2017
Source(s)	Bulletin de sécurité Cisco cisco-sa-20170124-webex du 24 janvier 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

2 - Systèmes affectés

le greffon Cisco WebEx pour Chrome Firefox et Internet Explorer sur Windows

3 - Résumé

Une vulnérabilité a été découverte dans *Cisco WebEx*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 - Solution

La vulnérabilité CVE-2017-3823 peut être exploitée lorsqu'un utilisateur se rend sur un site qui contient un motif particulier dans l'URL.
Comme ce motif peut être contenu dans une *iframe* qu'il est trivial de cacher, l'exploitation à l'insu de l'utilisateur est tout à fait possible.

Cisco annonce que seuls les systèmes Windows sont impactés par cette vulnérabilité.
Le greffon Cisco WebEx pour Edge sur Windows 10 n'est pas vulnérable.

Un correctif est disponible pour le greffon Cisco WebEx pour Chrome dans la version 1.0.5. Si celui-ci ne comble pas complètement la vulnérabilité, il en limite l'impact. En effet, si le motif particulier se trouve dans une URL associée à des domaines autres que `*.webex.com` ou `*.webex.com.cn`, l'utilisateur doit accepter explicitement l'exécution de code. Cependant, cela ne protège pas l'utilisateur si les sites susnommés sont vulnérables à des failles de type injection de code indirecte à distance (XSS).

Dans l'attente de correctifs de sécurité, le CERT-FR recommande la désinstallation du greffon Cisco Webex sur les systèmes vulnérables.
Lorsque cela n'est pas possible, le CERT-FR recommande a minima l'utilisation du greffon Cisco Webex par le biais d'un navigateur Chrome à jour.

Depuis le 31 janvier 2017, Cisco a publié un correctif de sécurité résolvant la vulnérabilité.

5 - Documentation

- Avis CERT-FR CERTFR-2017-AVI-036 Cisco WebEx Browser Extension
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-036/index.html
- Bulletin de sécurité Cisco cisco-sa-20170124-webex du 24 janvier 2017
  https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex
- Google Project Zero
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1096
- Référence CVE CVE-2017-3823
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3823

Gestion détaillée du document

25 janvier 2017 version initiale.
31 janvier 2017 clôture de l'alerte.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-001`