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 13 septembre 2017
N° CERTFR-2017-AVI-297

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans les produits Microsoft

Gestion du document

Référence	CERTFR-2017-AVI-297
Titre	Multiples vulnérabilités dans les produits Microsoft
Date de la première version	13 septembre 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 12 septembre 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)

- Divulgation d'informations
- Élévation de privilèges
- Exécution de code à distance

2 - Systèmes affectés

- ChakraCore
- Microsoft Exchange Server 2013 Cumulative Update 16
- Microsoft Exchange Server 2013 Cumulative Update 17
- Microsoft Exchange Server 2013 Service Pack 1
- Microsoft Exchange Server 2016 Cumulative Update 5
- Microsoft Exchange Server 2016 Cumulative Update 6
- Microsoft Live Meeting 2007 Add-in
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010 (32 bits)
- Microsoft Lync 2010 (64 bits)
- Microsoft Lync 2010 Attendee (installation niveau administrateur)
- Microsoft Lync 2010 Attendee (installation niveau utilisateur)
- Microsoft Lync 2013 Service Pack 1 (32 et 64 bits)

- Microsoft Lync Basic 2013 Service Pack 1 (32 et 64 bits)
- Microsoft Publisher 2007 Service Pack 3
- Microsoft Publisher 2010 Service Pack 2 (32 et 64 bits)
- Skype pour Business 2016 (32 et 64 bits)
- Skype pour Business 2016 Basic (32 et 64 bits)
- Xamarin.iOS

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Microsoft*. Elles permettent à un attaquant de provoquer une divulgation d'informations, une élévation de privilèges et une exécution de code 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 Microsoft du 12 septembre 2017
  https://portal.msrc.microsoft.com/fr-FR/security-guidance/advisory/
- Référence CVE CVE-2017-8758
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8758
- Référence CVE CVE-2017-8695
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8695
- Référence CVE CVE-2017-8696
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8696
- Référence CVE CVE-2017-8658
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8658
- Référence CVE CVE-2017-8676
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8676
- Référence CVE CVE-2017-8725
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8725
- Référence CVE CVE-2017-11761
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11761
- Référence CVE CVE-2017-8665
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8665

Gestion détaillée du document

13 septembre 2017 version initiale.

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-AVI-297`