

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Windows

Gestion du document

Référence	CERTFR-2016-AVI-271
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	10 août 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS16-097 du 09 août 2016 Bulletin de sécurité Microsoft MS16-102 du 09 août 2016 Bulletin de sécurité Microsoft MS16-098 du 09 août 2016 Bulletin de sécurité Microsoft MS16-100 du 09 août 2016 Bulletin de sécurité Microsoft MS16-101 du 09 août 2016 Bulletin de sécurité Microsoft MS16-103 du 09 août 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)

- exécution de code arbitraire à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Microsoft Windows Vista
- Microsoft Windows Server 2008
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2
- Microsoft Windows 8.1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows RT 8.1
- Microsoft Windows 10

- Skype Entreprise 2016
- Microsoft Lync 2013
- Microsoft Lync 2010
- Client Microsoft Live Meeting 2007
- Microsoft Office 2007
- Microsoft Office 2010
- Visionneuse Microsoft Word

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Microsoft Windows*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

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 MS16-097 du 09 août 2016
<https://technet.microsoft.com/fr-fr/library/security/MS16-097>
- Bulletin de sécurité Microsoft MS16-102 du 09 août 2016
<https://technet.microsoft.com/fr-fr/library/security/MS16-102>
- Bulletin de sécurité Microsoft MS16-098 du 09 août 2016
<https://technet.microsoft.com/fr-fr/library/security/MS16-098>
- Bulletin de sécurité Microsoft MS16-100 du 09 août 2016
<https://technet.microsoft.com/fr-fr/library/security/MS16-100>
- Bulletin de sécurité Microsoft MS16-101 du 09 août 2016
<https://technet.microsoft.com/fr-fr/library/security/MS16-101>
- Bulletin de sécurité Microsoft MS16-103 du 09 août 2016
<https://technet.microsoft.com/fr-fr/library/security/MS16-103>
- Référence CVE CVE-2016-3237
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3237>
- Référence CVE CVE-2016-3300
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3300>
- Référence CVE CVE-2016-3301
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3301>
- Référence CVE CVE-2016-3303
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3303>
- Référence CVE CVE-2016-3304
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3304>
- Référence CVE CVE-2016-3308
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3308>
- Référence CVE CVE-2016-3309
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3309>
- Référence CVE CVE-2016-3310
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3310>
- Référence CVE CVE-2016-3311
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3311>
- Référence CVE CVE-2016-3312
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3312>
- Référence CVE CVE-2016-3319
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3319>

- Référence CVE CVE-2016-3320
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3320>

Gestion détaillée du document

10 août 2016 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-2016-AVI-271>
