

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Office

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTFR-2017-AVI-147 |
| Titre | Multiples vulnérabilités dans Microsoft Office |
| Date de la première version | 10 mai 2017 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft mai 2017 du 09 mai 2017 Bulletin de sécurité Microsoft du 09 mai 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
- élévation de privilèges

2 - Systèmes affectés

- Microsoft Forefront Security for SharePoint Service Pack 3
- Microsoft Office 2007 Service Pack 3
- Microsoft Office 2010 Service Pack 2 (32-bit editions)
- Microsoft Office 2010 Service Pack 2 (64-bit editions)
- Microsoft Office 2013 RT Service Pack 1
- Microsoft Office 2013 Service Pack 1 (32-bit editions)
- Microsoft Office 2013 Service Pack 1 (64-bit editions)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 for Mac
- Microsoft Office Compatibility Pack Service Pack 3
- Microsoft Office Online Server 2016
- Microsoft Office Web Apps 2010 Service Pack 2

- Microsoft Office Web Apps 2013 Service Pack 1
- Microsoft Office Word Viewer
- Microsoft Office for Mac 2011
- Microsoft PowerPoint for Mac 2011
- Microsoft Project Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft SharePoint Server 2010 Service Pack 2
- Microsoft Word 2007 Service Pack 3
- Microsoft Word 2010 Service Pack 2 (32-bit editions)
- Microsoft Word 2010 Service Pack 2 (64-bit editions)
- Microsoft Word 2013 RT Service Pack 1
- Microsoft Word 2013 Service Pack 1 (32-bit editions)
- Microsoft Word 2013 Service Pack 1 (64-bit editions)
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Word Automation Services

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Microsoft Office*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges.

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 mai 2017 du 09 mai 2017
<https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/bc365363-f51e-e711-80da-000d3a32fc99>
- Bulletin de sécurité Microsoft du 09 mai 2017
<https://portal.msrc.microsoft.com/fr-FR/security-guidance>
- Référence CVE CVE-2017-0254
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0254>
- Référence CVE CVE-2017-0255
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0255>
- Référence CVE CVE-2017-0261
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0261>
- Référence CVE CVE-2017-0262
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0262>
- Référence CVE CVE-2017-0264
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0264>
- Référence CVE CVE-2017-0265
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0265>
- Référence CVE CVE-2017-0281
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0281>
- Référence CVE CVE-2017-0290
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290>

Gestion détaillée du document

10 mai 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-147>
