

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Windows

Gestion du document

Référence	CERTFR-2016-AVI-060
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	10 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS16-012 du 09 février 2016 Bulletin de sécurité Microsoft MS16-013 du 09 février 2016 Bulletin de sécurité Microsoft MS16-014 du 09 février 2016 Bulletin de sécurité Microsoft MS16-016 du 09 février 2016 Bulletin de sécurité Microsoft MS16-017 du 09 février 2016 Bulletin de sécurité Microsoft MS16-018 du 09 février 2016 Bulletin de sécurité Microsoft MS16-021 du 09 février 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
- déni de service à distance
- élévation de privilèges

2 - Systèmes affectés

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

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Microsoft Windows*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service 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 MS16-012 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-012>
- Bulletin de sécurité Microsoft MS16-013 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-013>
- Bulletin de sécurité Microsoft MS16-014 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-014>
- Bulletin de sécurité Microsoft MS16-016 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-016>
- Bulletin de sécurité Microsoft MS16-017 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-017>
- Bulletin de sécurité Microsoft MS16-018 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-018>
- Bulletin de sécurité Microsoft MS16-021 du 09 février 2016
<https://technet.microsoft.com/en-us/library/security/ms16-021>
- Référence CVE CVE-2016-0036
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0036>
- Référence CVE CVE-2016-0038
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0038>
- Référence CVE CVE-2016-0040
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0040>
- Référence CVE CVE-2016-0041
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0041>
- Référence CVE CVE-2016-0042
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0042>
- Référence CVE CVE-2016-0044
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0044>
- Référence CVE CVE-2016-0046
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0046>
- Référence CVE CVE-2016-0048
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0048>
- Référence CVE CVE-2016-0050
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0050>
- Référence CVE CVE-2016-0051
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0051>
- Référence CVE CVE-2016-0058
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0058>

Gestion détaillée du document

10 février 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-060>
