

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Windows

Gestion du document

Référence	CERTFR-2016-AVI-124
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	13 avril 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS16-040 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-044 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-045 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-046 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-047 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-048 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-049 du 12 avril 2016 Bulletin de sécurité Microsoft MS16-039 du 12 avril 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
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

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

- Windows Server 2012 R2
- Windows RT 8.1
- Windows 10

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 déni de service à distance et un contournement de la politique de sécurité.

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 MS16-040 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-040>
- Bulletin de sécurité Microsoft MS16-044 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-044>
- Bulletin de sécurité Microsoft MS16-045 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-045>
- Bulletin de sécurité Microsoft MS16-046 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-046>
- Bulletin de sécurité Microsoft MS16-047 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-047>
- Bulletin de sécurité Microsoft MS16-048 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-048>
- Bulletin de sécurité Microsoft MS16-049 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-049>
- Bulletin de sécurité Microsoft MS16-039 du 12 avril 2016
<https://technet.microsoft.com/fr-fr/library/security/ms16-039>
- Référence CVE CVE-2016-0088
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0088>
- Référence CVE CVE-2016-0089
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0089>
- Référence CVE CVE-2016-0090
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0090>
- Référence CVE CVE-2016-0128
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0128>
- Référence CVE CVE-2016-0135
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0135>
- Référence CVE CVE-2016-0143
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0143>
- Référence CVE CVE-2016-0145
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0145>
- Référence CVE CVE-2016-0147
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0147>
- Référence CVE CVE-2016-0150
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0150>
- Référence CVE CVE-2016-0151
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0151>
- Référence CVE CVE-2016-0153
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0153>

- Référence CVE CVE-2016-0165
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0165>
- Référence CVE CVE-2016-0167
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0167>

Gestion détaillée du document

13 avril 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-124>
