

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans Microsoft Windows

### Gestion du document

Référence	CERTFR-2016-AVI-230
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	12 juillet 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS16-086 du 12 juillet 2016 Bulletin de sécurité Microsoft MS16-087 du 12 juillet 2016 Bulletin de sécurité Microsoft MS16-089 du 12 juillet 2016 Bulletin de sécurité Microsoft MS16-090 du 12 juillet 2016 Bulletin de sécurité Microsoft MS16-092 du 12 juillet 2016 Bulletin de sécurité Microsoft MS16-094 du 12 juillet 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

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

### 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 MS16-086 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-086>
- Bulletin de sécurité Microsoft MS16-087 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-087>
- Bulletin de sécurité Microsoft MS16-089 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-089>
- Bulletin de sécurité Microsoft MS16-090 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-090>
- Bulletin de sécurité Microsoft MS16-091 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-091>
- Bulletin de sécurité Microsoft MS16-092 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-092>
- Bulletin de sécurité Microsoft MS16-094 du 12 juillet 2016  
<https://technet.microsoft.com/fr-fr/library/security/MS16-094>
- Référence CVE CVE-2016-3204  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3204>
- Référence CVE CVE-2016-3238  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3238>
- Référence CVE CVE-2016-3239  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3239>
- Référence CVE CVE-2016-3249  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3249>
- Référence CVE CVE-2016-3250  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3250>
- Référence CVE CVE-2016-3251  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3251>
- Référence CVE CVE-2016-3252  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3252>
- Référence CVE CVE-2016-3254  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3254>
- Référence CVE CVE-2016-3256  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3256>
- Référence CVE CVE-2016-3258  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3258>
- Référence CVE CVE-2016-3272  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3272>
- Référence CVE CVE-2016-3286  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3286>
- Référence CVE CVE-2016-3287  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3287>

## Gestion détaillée du document

12 juillet 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-230>

---