

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans le composant Microsoft Graphics**

### Gestion du document

Référence	CERTFR-2016-AVI-122
Titre	Multiples vulnérabilités dans le composant Microsoft Graphics
Date de la première version	13 avril 2016
Date de la dernière version	–
Source(s)	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
- élévation de privilèges

### 2 - Systèmes affectés

- Microsoft Windows
- Microsoft .NET Framework
- Microsoft Office
- Skype Entreprise
- Microsoft Lync

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *le composant Microsoft Graphics*. 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 MS16-039 du 12 avril 2016  
<https://technet.microsoft.com/fr-fr/library/security/ms16-039>
- 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-2016-0165  
<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-122>

---