

Affaire suivie par :  
CERT-FR

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTFR-2016-ACT-047**

### 1 - Fin de support de Microsoft Windows Vista

Microsoft a planifié l'arrêt du support de Microsoft Windows Vista le **11 avril 2017**. À cette date, l'éditeur cessera d'assurer la publication de correctifs de sécurité, y compris en cas de découverte d'une vulnérabilité critique. Il est important de souligner que l'arrêt du support de Windows Vista va entraîner une recrudescence des codes d'exploitation de vulnérabilité de type "0-day" dans les kits d'exploitation utilisés, notamment dans le cadre de menaces cybernétiques avancées. Ces vulnérabilités auront plus de valeur pour les attaquants dans la mesure où elles ne seront pas corrigées par l'éditeur. Le support et la mise à disposition de mises à jour de sécurité par l'éditeur sont un point crucial à la sécurisation d'un serveur ou d'une station de travail. L'arrêt du support d'une version de système d'exploitation doit être anticipé et constitue une motivation à la migration vers une version récente.

Cela concerne en majorité les postes de travail, mais peut également concerner des équipements intégrés embarquant le système Windows Vista (ex : équipements industriels, médicaux, interfaces utilisateurs, etc.).

Ces derniers pouvant faire l'objet de contraintes métier, une démarche spécifique doit être engagée, en coordination avec le fournisseur, afin d'étudier les différents scénarios envisageables. De plus, la durée de vie du système d'exploitation retenu pour la migration doit être adaptée au cycle de vie des projets et à la vitesse de renouvellement du parc informatique. Une période de cinq ans minimum est recommandée pour les environnements bureautiques. De nombreux systèmes utilisant Microsoft Windows Vista sont aujourd'hui encore en service. Le CERT-FR attire l'attention sur la nécessité d'anticiper dès à présent une migration vers des systèmes dont la sécurité pourra être assurée après le 11 avril 2017.

### 2 - Rappel des avis émis

Dans la période du 14 au 20 novembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-376 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-377 : Vulnérabilité dans VMware Workstation et Fusion
- CERTFR-2016-AVI-378 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-379 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-380 : Vulnérabilité dans les produits Symantec
- CERTFR-2016-AVI-381 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-382 : Multiples vulnérabilités dans Drupal
- CERTFR-2016-AVI-383 : Vulnérabilité dans SCADA les caméras IP-CCTV Siemens
- CERTFR-2016-AVI-384 : Multiples vulnérabilités dans SCADA Siemens SIMATIC CP 1543-1

# Gestion détaillée du document

21 novembre 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-ACT-047>

---