Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 11 février 2015
N° CERTFR-2015-AVI-061

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans le pilote en mode noyau de Microsoft Windows

Gestion du document

Référence	CERTFR-2015-AVI-061
Titre	Multiples vulnérabilités dans le pilote en mode noyau Microsoft Windows
Date de la première version	11 février 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS15-10 du 10 février 2015
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
- élévation de privilèges

2 - Systèmes affectés

- Windows Server 2003 Service Pack 2
- Windows Server 2003 Édition x64 Service Pack 2
- Windows Server 2003 avec SP2 pour systèmes Itanium
- Windows Vista Service Pack 2
- Windows Vista Édition x64 Service Pack 2
- Windows Server 2008 pour systèmes 32 bits Service Pack 2
- Windows Server 2008 pour systèmes x64 Service Pack 2
- Windows Server 2008 pour systèmes Itanium Service Pack 2
- Windows 7 pour systèmes 32 bits Service Pack 1
- Windows 7 pour systèmes x64 Service Pack 1
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1
- Windows 8 pour systèmes 32 bits
- Windows 8 pour systèmes x64

- Windows 8.1 pour systèmes 32 bits
- Windows 8.1 pour systèmes x64
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 (installation Server Core)
- Windows Server 2008 pour systèmes x64 Service Pack 2 (installation Server Core)
- Windows Server 2012 (installation Server Core)
- Windows Server 2012 R2 (installation Server Core)

3 - Résumé

De multiples vulnérabilités ont été corrigées dans le pilote en mode noyau de *Microsoft Windows*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité 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 MS15-10 du 10 février 2015
  https://technet.microsoft.com/fr-fr/library/security/MS15-010
- Référence CVE CVE-2015-0003
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0003
- Référence CVE CVE-2015-0010
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0010
- Référence CVE CVE-2015-0057
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0057
- Référence CVE CVE-2015-0058
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0058
- Référence CVE CVE-2015-0059
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0059
- Référence CVE CVE-2015-0060
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0060

Gestion détaillée du document

11 février 2015 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-2015-AVI-061`