

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le gestionnaire de files d'impression de Microsoft Windows

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-217>

Gestion du document

Référence	CERTA-2009-AVI-217
Titre	Vulnérabilités dans le gestionnaire de files d'impression de Microsoft Windows
Date de la première version	10 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-022 du 09 juin 2009
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

- Exécution de code arbitraire à distance ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

Microsoft Windows, toutes versions.

3 Résumé

Plusieurs vulnérabilités affectent le gestionnaire de files d'impression de Microsoft Windows permettant à un utilisateur malveillant d'exécuter du code arbitraire à distance, d'accéder à des informations sensibles ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités affectent le gestionnaire de files d'impression de Microsoft Windows (*Print Spooler*) :

- CVE-2009-0228 : une erreur de type débordement de zone mémoire est exploitable par un utilisateur malveillant, non authentifié, pour exécuter du code arbitraire sur l'ordinateur vulnérable ;
- CVE-2009-0229 : un défaut permet à un utilisateur malveillant, local et authentifié, sans devoir disposer de droits administrateur, de lire ou d'imprimer tout fichier sur le système vulnérable ;
- CVE-2009-0230 : un défaut dans la gestion des droits permet à un utilisateur malveillant, authentifié, d'élever ses privilèges puis de prendre le contrôle de l'ordinateur vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS09-022 du 09 juin 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-022.aspx>
<http://www.microsoft.com/technet/security/Bulletin/MS09-022.aspx>
- Référence CVE CVE-2009-0228 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0228>
- Référence CVE CVE-2009-0229 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0229>
- Référence CVE CVE-2009-0230 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0230>

Gestion détaillée du document

10 juin 2009 version initiale.