

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Windows Search

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-2008-AVI-589>

Gestion du document

Référence	CERTA-2008-AVI-589
Titre	Multiples vulnérabilités de Windows Search
Date de la première version	09 décembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-075 du 09 décembre 2008
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.

2 Systèmes affectés

- Windows Vista et Windows Vista Service Pack 1 ;
- Windows Vista et Windows Vista Service Pack 1 ;
- Windows Vista x64 Edition et Windows Vista x64 Service Pack 1 ;
- Windows Vista x64 Edition et Windows Vista x64 Service Pack 1 ;
- Windows Server 2008 pour les systèmes 32-bit ;
- Windows Server 2008 pour les systèmes x64 ;
- Windows Server 2008 pour les systèmes Itanium.

3 Résumé

Deux vulnérabilités présentes dans la fonction de recherche de Microsoft Windows Vista et Microsoft Windows Server 2008 permettent à un utilisateur distant malintentionné d'exécuter du code arbitraire.

4 Description

Deux erreurs sont présentes dans la fonction de recherche *Windows Search* de Microsoft Vista et Microsoft Server 2008. Ces vulnérabilités peuvent être exploitées par le biais d'un fichier de recherche sauvegardée ou *Saved Search* construit de façon particulière ou par le biais d'une URL pointant sur ce fichier. Elles permettent à un utilisateur distant malintentionné d'exécuter du code arbitraire.

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 MS08-075 du 09 décembre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-075.msp#>
<http://www.microsoft.com/technet/security/Bulletin/MS08-075.msp>
- Référence CVE CVE-2008-4268 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4268>
- Référence CVE CVE-2008-4269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4269>

Gestion détaillée du document

09 décembre 2008 version initiale.