

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft XML Core Services

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-550>

Gestion du document

Référence	CERTA-2008-AVI-550
Titre	Vulnérabilités dans Microsoft XML Core Services
Date de la première version	12 novembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-069 du 10 novembre 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Windows 2000 SP4, toutes éditions ;
- Windows Server 2003 SP1 et SP2, toutes éditions ;
- Windows XP SP2 et SP3, toutes éditions ;
- Windows Vista et Vista SP1, toutes éditions ;
- Windows Server 2008, toutes éditions ;
- Microsoft Office 2003 SP3, 2007, 2007 SP1 et Groove Server 2007 ;
- Word Viewer 2003 SP3 ;
- Compatibility Pack for 2007 file formats et Compatibility Pack SP1 ;
- Expression Web et Web 2 ;
- Sharepoint Server 2007 et 2007 SP1.

3 Résumé

Plusieurs vulnérabilités dans Microsoft XML Core Services permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance ou de porter atteinte à la confidentialité des données.

4 Description

Plusieurs vulnérabilités dans Microsoft XML Core Services ont été publiées :

- la lecture de pages ou de courriels HTML spécialement conçus provoque une corruption de mémoire. Cette vulnérabilité peut être exploitée par un utilisateur malveillant pour exécuter du code arbitraire à distance (CVE-2007-0099). Elle ne concerne que Microsoft XML CoreServices 3.0 ;
- un problème dans la gestion des DTD externes peut être exploité pour accéder à des informations d'un autre domaine dans Internet Explorer (CVE-2008-4029). Cette vulnérabilité ne concerne que Microsoft XML CoreServices 3.0 et 4.0 ;
- un problème dans le traitement des en-têtes peut être exploité pour accéder à des informations d'un autre domaine dans Internet Explorer (CVE-2008-4033). Cette vulnérabilité concerne toutes les versions.

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 MS08-069 du 10 novembre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-069.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS08-069.mspx>
- Référence CVE CVE-2007-0099 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0099>
- Référence CVE CVE-2008-4029 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4029>
- Référence CVE CVE-2008-4033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4033>

Gestion détaillée du document

12 novembre 2008 version initiale.