



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 15 novembre 2006
N° CERTA-2006-AVI-500

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2006-AVI-500>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2006-AVI-500 |
| Titre | Vulnérabilité de Microsoft XML Core Services |
| Date de la première version | 15 novembre 2006 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS06-071 du 14 novembre 2006 |
| 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft XML Core Services 4.0 (pour toutes les versions de Windows) ;
- Microsoft XML Core Services 6.0 (pour toutes les versions de Windows).

3 Résumé

Une vulnérabilité a été identifiée dans Microsoft XML Core Services (*MSXML*). Il s'agit plus précisément du contrôle ActiveX *XMLHTTP*.

Une personne malveillante pourrait exploiter cette vulnérabilité, afin de prendre le contrôle, à distance ou localement, de la machine fonctionnant sur un système vulnérable. Un scénario d'attaque possible serait une page Web construite de manière particulière : la visite de cette dernière par un navigateur autorisant les contrôles ActiveX, permettrait l'exécution de code sur le système.

Même si *MSXML* n'est pas distribué par défaut avec Windows, il est installé avec plusieurs logiciels.

4 Description

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 MS06-071 du 14 novembre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-071.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-071.msp>
- Avis de sécurité Microsoft 927892 du 03 novembre 2006 :
<http://www.microsoft.com/technet/security/advisory/927892.msp>
- Référence CVE CVE-2006-5745 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5745>

Gestion détaillée du document

15 novembre 2006 version initiale.