

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les composants Windows Media

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-590>

Gestion du document

Référence	CERTA-2008-AVI-590
Titre	Vulnérabilités dans les composants Windows Media
Date de la première version	09 décembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-076 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Lecteur Windows Media 6.4 ;
- module d'exécution du format Windows Media 7.1 ;
- module d'exécution du format Windows Media 9.0 ;
- module d'exécution du format Windows Media 9.5 ;
- module d'exécution du format Windows Media 11 ;
- Windows Media Services 4.1 ;
- Windows Media Services Série 9 ;
- Windows Media Services 2008.

3 Résumé

Plusieurs vulnérabilités dans les composants *Windows Media* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été corrigées dans les composants *Windows Media* :

- la première vulnérabilité concerne l'implémentation du *Service Principal Name* dans les composants *Windows Media* permettant la réflexion des informations d'identification NTLM et donc l'exécution de code arbitraire à distance (CVE-2008-3009) ;
- la deuxième vulnérabilité concerne l'implémentation du protocole ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) par des composants *Windows Media* (CVE-2008-3010). Une personne malintentionnée pourrait récupérer les informations d'identification NTLM d'un utilisateur en l'incitant à visiter une page spécialement conçue et à exécuter certaines actions.

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 MS08-076 du 09 décembre 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-076.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-076.msp>
- Référence CVE CVE-2008-3009 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3009>
- Référence CVE CVE-2008-3010 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3010>

Gestion détaillée du document

09 décembre 2008 version initiale.