



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 août 2008
N° CERTA-2008-AVI-410

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Windows Messenger

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-410>

Gestion du document

Référence	CERTA-2008-AVI-410
Titre	Vulnérabilité dans Windows Messenger
Date de la première version	13 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-050 du 12 août 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Windows Messenger 5.1 sur Windows 2000 SP4 et les versions 4.7 et 5.1 sur les systèmes suivants :

- Windows XP SP2 et SP3 ;
- Windows XP pro x64 et x64 SP2 ;
- Windows Server 2003 SP1 et SP2 (modéré) ;
- Windows Server 2003 x64 et x64 SP2 (modéré) ;
- Windows Server 2003 pour Itanium, SP1 et SP2 (modéré).

3 Résumé

Une vulnérabilité permet de manipuler Windows Messenger à l'insu de l'utilisateur connecté.

4 Description

Une vulnérabilité permet de contrôler `Windows Messenger` en utilisant des scripts pour manipuler un contrôle `ActiveX` et cela à l'insu de l'utilisateur connecté. Un attaquant peut, entre autres, en modifier l'état, démarrer la vidéo ou obtenir l'identifiant de l'utilisateur afin d'ouvrir une session à distance sur le client de messagerie à la place de l'utilisateur.

5 Solution

Se référer au bulletin de sécurité Microsoft MS08-050 de 12 août 2008 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-050 du 12 août 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-050.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-050.msp>
- Référence CVE CVE-2008-0082 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0082>

Gestion détaillée du document

13 août 2008 version initiale.