

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le système d'événements de Microsoft Windows

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-409>

Gestion du document

Référence	CERTA-2008-AVI-409
Titre	Multiples vulnérabilités dans le système d'événements de Microsoft Windows
Date de la première version	13 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-049 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Vista ;
- Microsoft Windows Server 2008.

3 Résumé

Plusieurs vulnérabilités affectant le système d'événements de *Microsoft Windows* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans le système d'événements de *Microsoft Windows* et permettent à une personne malveillante d'exécuter du code arbitraire à distance :

- une erreur dans la validation des demandes d'abonnements utilisateur par le système d'événements de *Microsoft Windows* permet à une personne malintentionnée d'exécuter du code arbitraire à distance ;
- une erreur dans la validation sur la plage d'index lors de l'appel d'un tableau de pointeurs de fonction par le système d'événements de *Microsoft Windows* permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

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 MS08-049 du 12 août 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-049.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-049.msp>
- Référence CVE CVE-2008-1456 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1456>
- Référence CVE CVE-2008-1457 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1457>

Gestion détaillée du document

13 août 2008 version initiale.