

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Macrovision SafeDisc

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-2007-AVI-480>

Gestion du document

Référence	CERTA-2007-AVI-480-001
Titre	Vulnérabilité dans Macrovision SafeDisc
Date de la première version	06 novembre 2007
Date de la dernière version	07 novembre 2007
Source(s)	Bulletin de sécurité Microsoft #944653 du 5 novembre 2007 Bulletin de sécurité Macrovision
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

Elévation de privilège.

2 Systèmes affectés

Macrovision SafeDisc 4.x.

Les systèmes d'exploitation suivants sont affectés par cette vulnérabilité :

- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows XP Professional x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 et système Itanium ;
- Microsoft Windows Server 2003 Service Pack 2 et système Itanium ;
- Microsoft Windows Server 2003 x64 Edition & Service Pack 2.

3 Résumé

Une vulnérabilité dans Macrovision SafeDisc permet à un utilisateur local malintentionné d'élever ses privilèges.

4 Description

Une vulnérabilité, de type débordement de mémoire, est causée par une erreur dans le traitement de certains arguments fournis en paramètre au pilote `secdrv.sys`.

Cette vulnérabilité, découverte dans `Macrovision SafeDisc`, permet à un utilisateur malveillant d'exécuter du code arbitraire avec les privilèges du système.

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 944653 du 05 novembre 2007 :
<http://www.microsoft.com/france/technet/security/advisory/944653.mspx>
- Bulletin de sécurité Macrovision :
<http://www.macrovision.com/promolanding/7352.htm>
- Référence CVE CVE-2007-5587 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5587>

Gestion détaillée du document

06 novembre 2007 version initiale.

07 novembre 2007 révision des risques liés à la vulnérabilité.