

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des outils Microsoft de protection

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-245>

Gestion du document

Référence	CERTA-2008-AVI-245
Titre	Vulnérabilités des outils Microsoft de protection
Date de la première version	14 mai 2008
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS08-029 du 13 mai 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

Déni de service à distance.

2 Systèmes affectés

- Microsoft Live OneCare ;
- Microsoft Antigen pour Exchange et pour SMTP Gateway ;
- Microsoft Windows Defender ;
- Microsoft Forefront Client security ;
- Microsoft Forefront Security pour Exchange ;
- Microsoft Forefront Security pour Sharepoint ;
- Microsoft System Sweeper, contenu dans Diagnostics and Recovery Toolset 6.0.

3 Résumé

Deux vulnérabilités affectant les produits *Microsoft* de protection contre les logiciels malveillants peuvent être exploitées par un utilisateur malveillant pour provoquer un déni de service à distance.

4 Description

Une première vulnérabilité provoque l'arrêt et le redémarrage du logiciel de protection lors du traitement d'un fichier malformé spécialement conçu.

La deuxième vulnérabilité provoque la saturation du disque et le redémarrage du logiciel de protection lors du traitement d'un fichier malformé spécialement conçu.

Chacune de ces vulnérabilités peut être exploitée par un utilisateur malveillant pour provoquer un déni de service 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 MS08-029 du 13 mai 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-029.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-029.msp>
- Référence CVE CVE-2008-1437 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1437>
- Référence CVE CVE-2008-1438 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1438>

Gestion détaillée du document

14 mai 2008 version initiale.