Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 août 2007
N° CERTA-2007-AVI-360

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Virtual PC et Virtual Server

Gestion du document

Référence	CERTA-2007-AVI-360
Titre	Vulnérabilité de Microsoft Virtual PC et Virtual Server
Date de la première version	14 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-049 du 14 août 2007
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 ;
- exécution de code arbitraire ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Virtual PC 2004 ;
- Microsoft Virtual PC 2004 Service Pack 1 ;
- Microsoft Virtual Server 2005 Standard Edition ;
- Microsoft Virtual Server 2005 Enterprise Edition ;
- Microsoft Virtual Server 2005 R2 Standard Edition ;
- Microsoft Virtual Server 2005 R2 Enterprise Edition ;
- Microsoft Virtual PC pour Mac version 6.1 ;
- Microsoft Virtual PC pour Mac version 7.

Les versions Microsoft Virtual PC 2007 et Microsoft Virtual Server 2005 R2 Service Pack 1 ne seraient pas affectées.

3 Résumé

Une vulnérabilité a été identifiée dans Microsoft Virtual PC et Microsoft Virtual Server. Cette dernière peut être exploitée par un utilisateur ayant accès à une machine virtuelle particulière pour exécuter du code sur le système d'accueil (hôte) ou sur d'autres machines virtuelles.

4 Description

Une vulnérabilité de type débordement de tas a été identifiée dans Microsoft Virtual PC et Microsoft Virtual Server. Cette dernière peut être exploitée par un utilisateur doté des droits administrateur sur le système d'exploitation invité afin d'exécuter du code sur le système d'exploitation hôte ou sur d'autres systèmes invité.

5 Solution

Se référer au bulletin de sécurité MS07-049 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-049 du 14 août 2007 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS07-049.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-049.mspx
- Référence CVE CVE-2007-0948 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0948

Gestion détaillée du document

14 août 2007 version initiale.