



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 septembre 2008
N° CERTA-2008-AVI-445

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits VMware

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-445>

Gestion du document

Référence	CERTA-2008-AVI-445
Titre	Multiples vulnérabilités dans les produits VMware
Date de la première version	05 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin VMsa-2008-0014 du 30 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 ;
- exécution de code arbitraire ;
- déni de service à distance ;
- déni de service ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- VMware Server 1.x ;
- VMware ACE 1.x ;
- VMWare ACE 2.x ;
- VMware Player 1.x ;
- VMWare Player 2.x ;
- VMware Workstation 5.x ;
- VMware Workstation 6.x.

3 Résumé

Plusieurs vulnérabilités sont présentes dans les produits VMware. Certaines permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent les produits VMware :

- l'utilitaire de sauvegarde en ligne de commande, VMware Consolidated Backup, présente un défaut de protection des mots de passe ;
- une vulnérabilité dans la fonction *OpenProcess* est exploitable par un utilisateur local malveillant pour élever ses privilèges ;
- l'exploitation de vulnérabilités dans des ActiveX permet l'exécution de code arbitraire à distance, sur des produits fonctionnant sous Windows ;
- une extension de l'interface de programmation ISAPI de VMware server sous Windows présente un défaut. Son exploitation permet à un utilisateur malveillant de provoquer un déni de service à distance, dans certaines configurations de IIS ;
- une vulnérabilité de FreeType permet à un utilisateur malveillant d'exécuter du code arbitraire ;
- une vulnérabilité de Cairo permet à un utilisateur malveillant d'exécuter du code arbitraire par le biais d'un fichier image PNG spécifiquement conçu ;
- une vulnérabilité de libpng permet à un utilisateur malveillant de provoquer un arrêt inopiné du système par le biais d'un fichier image PNG spécifiquement conçu ;

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité VMSA-2008-0014 du 30 août 2008 :
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>
- Référence CVE CVE-2007-5269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5269>
- Référence CVE CVE-2007-5438 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5438>
- Référence CVE CVE-2007-5503 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5503>
- Référence CVE CVE-2008-1447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447>
- Référence CVE CVE-2008-1806 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1806>
- Référence CVE CVE-2008-1807 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1807>
- Référence CVE CVE-2008-1808 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1808>
- Référence CVE CVE-2008-2101 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2101>
- Référence CVE CVE-2008-3691 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3691>
- Référence CVE CVE-2008-3692 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3692>
- Référence CVE CVE-2008-3693 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3693>

- Référence CVE CVE-2008-3694 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3694>
- Référence CVE CVE-2008-3695 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3695>
- Référence CVE CVE-2008-3696 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3696>
- Référence CVE CVE-2008-3697 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3697>
- Référence CVE CVE-2008-3698 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3698>

Gestion détaillée du document

05 septembre 2008 version initiale.