

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans VMware ESX

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-2010-AVI-583>

Gestion du document

Référence	CERTA-2010-AVI-583
Titre	Multiples vulnérabilités dans VMware ESX
Date de la première version	09 décembre 2010
Date de la dernière version	–
Source(s)	Avis de sécurité VMware VMSA-2010-0019 du 07 décembre 2010
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 ;
- exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- VMware ESX 4.x Console OS (COS) ;
- VMware ESX 3.x Console OS (COS).

3 Résumé

De multiples vulnérabilités affectant différents logiciels inclus dans VMware ESX Console OS ont été corrigées.

4 Description

Plusieurs logiciels vulnérables inclus dans VMware ESX Console OS ont été mis à jour par l'éditeur :

- Samba est mis à jour pour corriger une vulnérabilité permettant à un utilisateur malveillant distant de provoquer un déni de service et potentiellement de l'exécution de code arbitraire (CVE-2010-3069) ;
- `bz_iP2` est mis à jour pour corriger une vulnérabilité permettant à un attaquant d'exécuter du code arbitraire à l'aide d'un fichier spécialement conçu (CVE-2010-0405) ;
- OpenSSL est mis à jour pour corriger plusieurs vulnérabilités permettant de contourner la politique de sécurité (CVE-2009-0590, CVE-2009-2409 et CVE-2009-3555).

5 Solution

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

6 Documentation

- Bulletin de sécurité VMware VMSA-2010-0019 du 07 décembre 2010 :
<http://www.vmware.com/security/advisories/VMSA-2010-0019.html>
- Référence CVE CVE-2010-3069 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3069>
- Référence CVE CVE-2010-0405 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0405>
- Référence CVE CVE-2009-0590 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0590>
- Référence CVE CVE-2009-2409 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2409>
- Référence CVE CVE-2009-3555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>

Gestion détaillée du document

09 décembre 2010 version initiale.