

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans XEN

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-532>

Gestion du document

Référence	CERTA-2007-AVI-532
Titre	Vulnérabilité dans Xen
Date de la première version	07 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Xen du 22 octobre 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.

2 Systèmes affectés

Xen versions antérieures à la version 3.1.2 fonctionnant sur les architectures IA64.

3 Résumé

Une vulnérabilité permettant de contourner la politique de sécurité a été découverte dans Xen.

4 Description

Une vulnérabilité a été découverte dans le logiciel de virtualisation Xen. Cette vulnérabilité présente dans la fonction `mov_to_rr()` peut être exploitée par un utilisateur mal intentionné afin de contourner les mécanismes de sécurité et de lire la mémoire d'un domaine VT-i depuis un autre domaine VT-i.

5 Solution

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

6 Documentation

- Bulletin de sécurité Xen du 22 Octobre 2007 :
<http://lists.xensource.com/archives/html/xen-ia64-devel/2007-10/msg00189.html>
- Référence CVE CVE-2007-6207 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6207>

Gestion détaillée du document

07 décembre 2007 version initiale.