

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans l'hyperviseur 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-2011-AVI-628>

Gestion du document

Référence	CERTA-2011-AVI-628
Titre	Multiples vulnérabilités dans l'hyperviseur <i>Xen</i>
Date de la première version	14 novembre 2011
Date de la dernière version	–
Source(s)	Bulletin d'alerte Debian DSA-2337-1 du 06 novembre 2011
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 ;
- élévation de privilèges.

2 Systèmes affectés

- *Xen* version 3.x ;
- *Xen* version 4.x.

3 Résumé

De multiples vulnérabilités ont été corrigées dans l'hyperviseur *Xen*.

4 Description

- CVE-2011-1166 : une machine virtuelle (VM) 64-bits peut placer un de ses microprocesseurs (*vCPU*) en mode non-noyau sans au préalable avoir fourni une table des pages non-noyau valide ;

- CVE-2011-1583, CVE-2011-3262 : la fonction qui interprète l'image noyau d'une VM paravirtualisée contient des vulnérabilités. Des utilisateurs locaux peuvent provoquer un déni de service ou exécuter du code arbitraire à l'aide une image noyau spécialement conçue d'une VM paravirtualisée ;
- CVE-2011-1898 : une vulnérabilité est présente lorsqu'une puce *Intel VT-d* sans mécanisme d'isolation des interruptions (*interrupt remapping*) est utilisée pour passer le contrôle de dispositifs PCI à une VM (*PCI passthrough*). Un utilisateur de la VM pourrait écrire dans les registres d'injection d'interruption et obtenir le contrôle sur le système d'exploitation hôte.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 2337-1 du 06 novembre 2011 :
<http://www.debian.org/security/2011/dsa-2337-1>
- Référence CVE CVE-2011-1166 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1166>
- Référence CVE CVE-2011-1583 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1583>
- Référence CVE CVE-2011-3262 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3262>
- Référence CVE CVE-2011-1898 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1898>

Gestion détaillée du document

14 novembre 2011 version initiale.