

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Qemu

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-383>

Gestion du document

Référence	CERTA-2011-AVI-383
Titre	Vulnérabilité dans Qemu
Date de la première version	07 juillet 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité RedHat RHSA-2011-0919 du 05 juillet 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

- Déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Qemu-kvm versions inférieures à 0.14

3 Résumé

Deux vulnérabilités ont été corrigées dans *qemu-kvm* et permettent à un utilisateur d'un système invité, de réaliser un déni de service et dans certains cas, d'élèver ses privilèges dans le système hôte.

4 Description

Deux vulnérabilités dans *qemu-kvm* ont été corrigées. La première (CVE-2011-2212) permet à un utilisateur avec privilèges sur un système invité, de réaliser un déni de service et dans certains cas, d'élèver ses privilèges sur le système hôte, au moyen d'un débordement de tampon. La seconde (CVE-2011-2512) permet à un utilisateur

d'un système invité, sans privilèges sur ce système, de réaliser un déni de service et dans certains cas, d'élever ses privilèges sur le système hôte, via une erreur de manipulation d'index de tableau.

5 Solution

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

6 Documentation

- Bulletin de sécurité RedHat RHSA-2011-0919 du 05 juillet 2011 :
<http://rhn.redhat.com/errata/RHSA-2011-0919.html>
- Référence CVE CVE-2011-2212 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2212>
- Référence CVE CVE-2011-2512 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2512>

Gestion détaillée du document

07 juillet 2011 version initiale.