Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 août 2008
N° CERTA-2008-AVI-429

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Xen

Gestion du document

Référence	CERTA-2008-AVI-429
Titre	Vulnérabilité de Xen
Date de la première version	27 août 2008
Date de la dernière version	–
Source(s)	Bulletin de mise à jour Xen du 21 juillet 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 en local ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Xen versions 3.3 et antérieures.

3 Résumé

Une vulnérabilité a été découverte dans le logiciel de virtualisation Xen. L'exploitation de cette vulnérabilité permet à un utilisateur malintentionné de réaliser un déni de service local ou de contourner la politique de sécurité.

4 Description

Une vulnérabilité a été découverte dans la gestion des appels *flask_op*. L'exploitation de cette vulnérabilité provoque un débordement de tas qu'une personne malintentionnée peut utiliser afin d'exécuter du code arbitraire sous les privilèges *Dom0*.

Seules les versions de Xen compilées avec la prise en charge du module `XSM:FLASK` sont vulnérables.

5 Solution

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

6 Documentation

- Mise à jour différentielle de Xen 21 juillet 2008 :
  http://xenbits.xensource.com/xen-3.3-testing.hq?rev/fa66b33f975a
- Référence CVE CVE-2008-3687 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3687

Gestion détaillée du document

27 août 2008 version initiale.