

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Vim

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-225>

Gestion du document

Référence	CERTA-2007-AVI-225-001
Titre	Vulnérabilité dans Vim
Date de la première version	24 mai 2007
Date de la dernière version	29 mai 2007
Source(s)	Bulletin de sécurité RedHat du 09.05.2007
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

– Exécution de code arbitraire ;

2 Systèmes affectés

Vim versions 7.0.219 et antérieures.

3 Résumé

Une vulnérabilité dans l'éditeur de texte Vim permet d'exécuter du code arbitraire.

4 Description

Une erreur dans la fonction *feedkeys()* de l'éditeur de texte Vim permet à un utilisateur malintentionné d'exécuter du code arbitraire dans le contexte d'un éditeur vulnérable par le biais d'un fichier construit de façon particulière. L'exploitation de la vulnérabilité nécessite que l'option *modelines* soit activée dans Vim.

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2007:101 du 09 mai 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:101>
- Bulletin de sécurité RedHat RHSA-2007:0346 du 09 mai 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0346.html>
- Bulletin de sécurité Ubuntu USN-463-1 du 22 mai 2007 :
<http://www.ubuntulinux.org/usn/usn-463-1>
- Bulletin de sécurité SuSE SUSE-SR:2007:012 :
<http://lists.suse.com/archive/suse-security-announce/2007-May/0008.html>
- Référence CVE CVE-2007-2438 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2438>

Gestion détaillée du document

24 mai 2007 version initiale.

29 mai 2007 ajout de la référence au bulletin de sécurité SuSE.