



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 mars 2005
N° CERTA-2005-AVI-068-003

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-2005-AVI-068>

Gestion du document

Référence	CERTA-2005-AVI-068-003
Titre	Vulnérabilité dans vim
Date de la première version	11 février 2005
Date de la dernière version	01 mars 2005
Source(s)	Bulletin de sécurité Mandrake MDKSA-2005:029
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Elévation des privilèges ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

Vim 6.x.

3 Résumé

Une vulnérabilité dans le binaire vim permet à un utilisateur local mal intentionné d'élever ses privilèges et de porter atteinte à l'intégrité des données présentes sur le système vulnérable.

4 Description

L'application vim est un éditeur de texte, présent dans de nombreuses distributions de Linux et Unix. Les scripts `tchtags` et `vimspell.sh` utilisés par vim sont vulnérables à une attaque qui permet l'écrasement de fichiers via le suivi des liens symboliques. A l'aide de liens habilement constitués, un utilisateur mal intentionné, ayant un accès local au système, peut forcer la modification de fichiers avec les droits de la victime.

5 Solution

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

6 Documentation

- Bulletin de sécurité Mandrake MDKSA-2005:029 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:029>
- Bulletin de sécurité RedHat RHSA-2005:036 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-036.html>
- Bulletin de sécurité RedHat RHSA-2005:122 du 18 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-122.html>
- Correctifs de sécurité pour Fedora Core 2 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Correctifs de sécurité pour Fedora Core 3 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Mise à jour de sécurité du paquetage NetBSD vim-share :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/vim-share/README.html>
- Référence CVE CAN-2005-0069 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0069>

Gestion détaillée du document

11 février 2005 version initiale.

17 février 2005 ajout de la référence au bulletin de sécurité RedHat.

21 février 2005 ajout de la référence au bulletin de sécurité RedHat.

01 mars 2005 ajout de la référence au bulletin de sécurité NetBSD.