

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'éditeur 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-292>

Gestion du document

Référence	CERTA-2005-AVI-292-002
Titre	Vulnérabilité de l'éditeur Vim
Date de la première version	29 juillet 2005
Date de la dernière version	31 août 2005
Source(s)	Avis de sécurité #75 de Georgi Guninski
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 avec les privilèges de l'utilisateur courant.

2 Systèmes affectés

Vim peut être utilisé sur de nombreux systèmes depuis les Unix jusqu'aux systèmes Microsoft en passant par les Macintoshs.

3 Description

Vim est un éditeur de texte pouvant recevoir des commandes. Ces commandes peuvent être insérées dans le corps même des fichiers édités. Une mauvaise gestion de certaines commandes permet l'exécution de commandes « shell » arbitraires incluses dans un document malicieux si l'option « modelines » est activée.

Les versions graphiques `kvim`, `gvim`,... sont également affectées.

4 Solution

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

5 Documentation

- Site internet de Vim (utiliser la révision 6.3.082 au moins) :
<http://www.vim.org/>
- Liste des correctifs de la version 6.3 de Vim :
<ftp://ftp.vim.org/pub/vim/patches/6.3/README>
- La version 6.3.084 est stable sous Gentoo Linux quelle que soit l'architecture depuis le 23 juillet 2005.
- Bulletin de sécurité RedHat RHSA-2005-745 du 22 août 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-745.html>
- Bulletin de sécurité Mandriva MDKSA-2005:148 du 22 août 2005 :
<http://www.mandriva.com/security/advisories/name=MDKSA-2005:148>
- Bulletin de sécurité Avaya ASA-2005-189 du 31 août 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-189.pdf>
- Bulletin de sécurité OpenBSD du 27 juillet 2005 :
<http://www.vuxml.org/openbsd/7d55ff5a-ffa7-11d9-a07e-000b5d77b0f5.html>
- Mise à jour NetBSD du paquetage Vim :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/vim/README.html>
- Avis de sécurité #75 de Georgi Guninski du 25 juillet 2005 :
http://www.guninski.com/where_do_you_want_billg_to_go_today_5.html
- Bulletins de sécurité FreeBSD pour vim, vim+ruby et vim-lite du 31 juillet 2005 :
<http://www.vuxml.org/openbsd/pkg-vim.html>
<http://www.vuxml.org/openbsd/pkg-vim+ruby.html>
<http://www.vuxml.org/openbsd/pkg-vim-lite.html>
- Référence CVE CAN-2005-2368 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2368>

Gestion détaillée du document

29 juillet 2005 version initiale.

01 août 2005 ajout des références aux bulletins de sécurité FreeBSD.

31 août 2005 ajout des références aux bulletins de sécurité RedHat, Mandriva et Avaya.