Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 mars 2009
N° CERTA-2009-AVI-101

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans vim

Gestion du document

Référence	CERTA-2009-AVI-101
Titre	Multiples vulnérabilités dans vim
Date de la première version	18 mars 2009
Date de la dernière version	–
Source(s)	Annonce du lancement de la version 7.2 de vim du 09 août 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 à distance.

2 Systèmes affectés

Toutes les versions de vim antérieures à 7.2.

3 Résumé

Plusieurs vulnérabilités de `vim` permettent à un individu malintentionné d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités de `vim` ont été découvertes :

– la première (CVE-2007-2953) concerne un défaut de validation des données fournies à la commande *helptags* ;

– la seconde (CVE-2008-2712) concerne un défaut de validation d'arguments lors d'appel système par un script `vim` ;
– la troisième (CVE-2008-3074) concerne un manque de validation des noms de fichier par l'extension *tar* de `vim` ;
– la quatrième (CVE-2008-3075) concerne un manque de validation des noms de fichier par l'extension *zip* de `vim` ;
– la cinquième (CVE-2008-3076 et CVE-2008-6235) concerne un manque de validation des noms de fichier par l'extension *netrw* de `vim` ;
– la dernière (CVE-2008-4101) vient d'un défaut de contrôle des caractères par la fonctionnalité de recherche de mots clef.

Toutes ces vulnérabilités permettent à un individu malintentionné d'exécuter du code arbitraire à distance par le biais d'un fichier spécialement construit ou en invitant un utilisateur à exécuter des commandes `vim` spécifiques.

5 Solution

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

6 Documentation

– Annonce du lancement de la version 7.2 de vim du 09 août 2008 :
http://groups.google.com/group/vim_announce/browse_thread/thread/2c89671dd928812f
– Bulletin de sécurité Debian DSA 1733 du 03 mars 2009 :
http://www.debian.org/security/2009/dsa-1733
– Bulletin de sécurité RedHat RHSA-2008:0580 du 25 novembre 2008 :
http://rhn.redhat.com/errata/RHSA-2008-0580.html
– Référence CVE CVE-2007-2953 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2953
– Référence CVE CVE-2008-2712 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2712
– Référence CVE CVE-2008-3074 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3074
– Référence CVE CVE-2008-3075 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3075
– Référence CVE CVE-2008-3076 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3076
– Référence CVE CVE-2008-4101 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4101
– Référence CVE CVE-2008-6235 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-6235

Gestion détaillée du document

18 mars 2009 version initiale.