Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 août 2006
N° CERTA-2005-AVI-190-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de divers outils gérant le format ELF

Gestion du document

Référence	CERTA-2005-AVI-190-003
Titre	Vulnérabilité de divers outils gérant le format ELF
Date de la première version	03 juin 2005
Date de la dernière version	02 août 2006
Source(s)	
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

- Elévation de privilèges ;
- exécution de code arbitraire avec les droits de l'utilisateur courant.

2 Systèmes affectés

Tout système Unix utilisant les paquetages GNU suivants :
- *gdb*,
- *binutils* (contenant les programmes *strings*, *nm*, *objdump*,...),
- *elfutils*,
- *HT Editor*.

3 Description

ELF est une spécification de format binaire utilisé pour les exécutables et les bibliothèques partagées. C'est maintenant le format utilisé dans Solaris, Linux et les BSDs (OpenBSD, FreeBSD et NetBSD).

Une mauvaise gestion de la mémoire, dans divers utilitaires analysant ce format, permet à un utilisateur mal intentionné de faire exécuter par sa victime du code arbitraire à l'aide d'un fichier *ELF* volontairement mal formé.

Par ailleurs, un mauvais choix de conception dans *gdb* permet l'exécution de tout fichier *.gdbinit* présent dans le répertoire courant et donc de lancer des commandes arbitraires avec les privilèges de l'utilisateur.

gdb est un débogueur, *binutils* contient entre autres *strings* qui permet d'extraire les chaînes de caractères d'un fichier, *elfutils* regroupe des utilitaires spécifiquement dédiés au format *elf* et *HT Editor* est un éditeur de fichiers exécutables.

4 Solution

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

5 Documentation

- Site de *gdb* :
  http://www.gnu.org/software/gdb/ ou
  http://sources.redhat.com/gdb/
- Site de *HT Editor* (version source 0.9.0 au moins) :
  http://hte.sourceforge.net/
- Site du paquetage *binutils* :
  http://sources.redhat.com/binutils/
- Site du paquetage *elfutils* :
  http://people.redhat.com/drepper/
- Bulletins de sécurité Gentoo :
  - GLSA-200505-08 du 10 mai 2005 pour *HT Editor* :
    http://www.gentoo.org/security/en/glsa/glsa-200505-08.xml
  - GLSA-200505-15 du 20 mai 2005 pour *gdb* :
    http://www.gentoo.org/security/en/glsa/glsa-200505-15.xml
  - GLSA-200506-01 du 1er juin 2005 pour *binutils* et *elfutils*:
    http://www.gentoo.org/security/en/glsa/glsa-200506-01.xml
- Bulletin de sécurité Mandriva MDKSA-2005:095 du 30 mai 2005 pour *gdb* :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005-095
- Bulletin de sécurité RedHat RHSA-2005:709 du 05 octobre 2005 pour *gdb* :
  http://rhn.redhat.com/errata/RHSA-2005-709.html
- Mise à jour NetBSD de *gdb* :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/devel/gdb/README.html
- Bulletin de sécurité Mandriva MDKSA-2005:215 du 24 novembre 2005 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2005-215
- Bulletin de sécurité SGI 20060703-01-P du 31 juillet 2006 :
  ftp://patches.sgi.com/support/free/security/advisories/20060703-01-U.asc
- Référence CVE CAN-2005-1545 pour *HT Editor* :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-1545
- Référence CVE CAN-2005-1704 pour *gdb* :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-1704
- Référence CVE CAN-2005-1705 pour *gdb* :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-1705

Gestion détaillée du document

03 juin 2005 version initiale ;

7 octobre 2005 ajout de la référence au bulletin de sécurité RedHat.

24 novembre 2005 ajout de la référence au bulletin de sécurité Mandriva.

02 août 2006 ajout de la référence au bulletin de sécurité SGI.