

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Gnu GCC

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-2006-AVI-300>

Gestion du document

Référence	CERTA-2006-AVI-300-001
Titre	Vulnérabilité dans Gnu GCC
Date de la première version	19 juillet 2006
Date de la dernière version	11 septembre 2006
Source(s)	Rapport d'erreur #28359 du projet gcc du 17 juillet 2006
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

Atteinte à l'intégrité des données.

2 Systèmes affectés

- Gnu GCC versions 3.x ;
- Gnu GCC versions 4.x.

3 Résumé

Une vulnérabilité dans Gnu GCC permet à un utilisateur mal intentionné de porter atteinte à l'intégrité des données du système.

4 Description

Gnu GCC est un compilateur libre pour différents langages comme C ou C++ mais aussi Java. Une erreur est présente dans un composant de Gnu GCC nommé `fastjar` mettant en œuvre la gestion des fichiers archive de type JAR (Java Archive). Cette vulnérabilité permet à un utilisateur mal intentionné d'écraser des fichiers

du système par ceux présents dans l'archive par une technique de type « traversée de repertoire » au moyen d'un fichier JAR construit de façon particulière.

5 Solution

Appliquer le correctif approprié :

<http://gcc.gnu.org/bugzilla/attachment.cgi?id=11904&action=view>

6 Documentation

- Site de Gnu GCC :
<http://gcc.gnu.org>
- Rapport d'erreur #28359 du projet gcc du 17 juillet 2006 :
http://gcc.gnu.org/bugzilla/show_bug.cgi?id=28359
- Bulletin de sécurité Debian DSA-1170 du 06 septembre 2006 :
<http://www.debian.org/security/2006/dsa-1170>
- Référence CVE CVE-2006-3619 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3619>

Gestion détaillée du document

19 juillet 2006 version initiale.

11 septembre 2006 ajout de la référence au bulletin de sécurité Debian.