



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juin 2009
N° CERTA-2009-AVI-244

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de APR-util

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-2009-AVI-244>

Gestion du document

Référence	CERTA-2009-AVI-244
Titre	Multiples vulnérabilités de APR-util
Date de la première version	19 juin 2009
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 1.3.7 de APR-util
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

- Dénis de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- toutes les versions de APR-util antérieures à 1.3.5 : CVE-2009-0023 et CVE-2009-1956 ;
- toutes les versions de APR-util antérieures à 1.3.7 : CVE-2009-1955.

3 Résumé

Plusieurs vulnérabilités présentes dans APR-util permettent à un utilisateur distant de provoquer un déni de service ou de porter atteinte à la confidentialité de certaines données.

4 Description

APR-util (Apache Portable Runtime) est une bibliothèque de fonctions constituant un socle commun et multi-plateforme d'outils sur lesquels s'appuie le serveur Web Apache pour fonctionner. Trois vulnérabilités sont présentes dans cette bibliothèque :

- La première (CVE-2009-1955) est relative à la manipulation des fichiers au format XML et permet à un utilisateur distant de provoquer un déni de service par le biais d'un fichier XML particulier ;
- la seconde (CVE-2009-0023) concerne la fonction *apr_strmatch_precompile()* et permet à un utilisateur distant de provoquer un déni de service ;
- la dernière (CVE-2009-1956) est présente dans la fonction *apr_brigade_vprintf()* et permet à un utilisateur distant de provoquer un déni de service ou d'obtenir un contenu partiel de la mémoire.

5 Solution

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

6 Documentation

- liste des changements apportés aux versions 1.3.5 et 1.3.7 de APR-util :
<http://www.apache.org/dist/apr/CHANGES-APR-UTIL-1.3>
- Bulletin de sécurité Debian DSA 1812 du 04 juin 2009 :
<http://www.debian.org/security/2009/dsa-1812>
- Bulletin de sécurité Mandriva MDVSA-2009:131 du 06 juin 2009 :
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité Ubuntu USN-786-1 du 10 juin 2009 :
<http://www.ubuntulinux.org/usn/usn-786-1>
- Référence CVE CVE-2009-0023 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0023>
- Référence CVE CVE-2009-1955 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1955>
- Référence CVE CVE-2009-1956 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1956>

Gestion détaillée du document

19 juin 2009 version initiale.