

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans cfengine

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-384>

Gestion du document

Référence	CERTA-2005-AVI-384-002
Titre	Multiples vulnérabilités dans cfengine
Date de la première version	07 octobre 2005
Date de la dernière version	14 octobre 2005
Source(s)	Bulletin de sécurité Debian DSA-835 du 01 octobre 2005 Bulletin de sécurité Debian DSA-836 du 01 octobre 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Elévation de privilèges ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- cfengine 1.6.5 et versions antérieures ;
- cfengine 2.1.16 et versions antérieures.

3 Résumé

Deux vulnérabilités découvertes dans l'application cfengine permettent à un utilisateur local mal intentionné d'élever ses privilèges et de porter atteinte à l'intégrité des données.

4 Description

`cfengine` est outil permettant d'administrer automatiquement un parc de machine.

Les scripts `vicf.in`, `cfmailfilter` et `cfcron.in` utilisés par `cfengine` sont vulnérables à une attaque qui permet l'écrasement de fichiers via le suivi des liens symboliques. A l'aide de liens habilement constitués, un utilisateur mal intentionné, ayant un accès local au système, peut forcer la modification de fichiers avec les droits de la victime.

5 Solution

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

6 Documentation

- Site internet de l'éditeur :
<http://www.cfengine.org/>
- Bulletin de sécurité Debian DSA-835 01 octobre 2005 :
<http://www.debian.org/security/2005/dsa-835>
- Bulletin de sécurité Debian DSA-836 01 octobre 2005 :
<http://www.debian.org/security/2005/dsa-836>
- Bulletin de sécurité Mandriva MDKSA-2005:184 13 octobre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:184>
- Bulletin de sécurité Ubuntu USN-198-1 du 10 octobre 2005 :
<http://www.ubuntu.com/usn/usn-198-1>
- Référence CVE CAN-2005-2960 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2960>
- Référence CVE CAN-2005-3137 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3137>

Gestion détaillée du document

07 octobre 2005 version initiale.

11 octobre 2005 ajout des références au bulletin de sécurité Ubuntu USN-198-1 et CVE CAN-2005-3137.

14 octobre 2005 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:184.