



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 juin 2004
N° CERTA-2004-AVI-141-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'application utempter

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-2004-AVI-141>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2004-AVI-141-004 |
| Titre | Vulnérabilité de l'application utempter |
| Date de la première version | 23 avril 2004 |
| Date de la dernière version | 09 juin 2004 |
| Source(s) | Avis de sécurité Mandrake MDKSA-2004:031 |
| 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.

2 Systèmes affectés

utempter versions 0.5.x.

3 Résumé

Une vulnérabilité présente dans *utempter* permet à un utilisateur mal intentionné d'exécuter des commandes avec des privilèges élevés.

4 Description

utempter est une application qui peut être utilisée pour mettre à jour les fichiers */var/run/utmp* et */var/log/wtmp*.

Une vulnérabilité de l'application permet à un utilisateur mal intentionné, en utilisant un lien symbolique, d'écraser un fichier avec les droits de l'administrateur *root*.

5 Solution

Appliquer le correctif fourni par votre éditeur.

6 Documentation

- Avis de sécurité Mandrake MDKSA-2004:031 du 19 avril 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:031>
- Avis de sécurité RedHat RHSA-2004:174 du 26 mai 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-174.html>
- Avis de sécurité RedHat RHSA-2004:175 du 30 avril 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-175.html>
- Avis de sécurité Gentoo GLSA 200405-05 du 13 mai 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200405-05.xml>
- Avis de sécurité SUSE SuSE-SA:2004:012 du 14 mai 2004 :
http://www.suse.com/de/security/2004_12_mc.html
- Référence CVE CAN-2004-0233 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0233>

Gestion détaillée du document

23 avril 2004 version initiale.

03 mai 2004 ajout de l'avis de sécurité RedHat.

14 mai 2004 ajout de l'avis de sécurité Gentoo.

17 mai 2004 correction des références Mandrake et Gentoo, ajout de l'avis de sécurité SUSE.

09 juin 2004 ajout d'un second avis de sécurité RedHat.