

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Usermin

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-306>

Gestion du document

Référence	CERTA-2004-AVI-306-004
Titre	Vulnérabilité de Usermin
Date de la première version	09 septembre 2004
Date de la dernière version	23 septembre 2004
Source(s)	Bulletin de sécurité SNS No.77 du 07 septembre 2004
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 ;
- exécution de code arbitraire.

2 Systèmes affectés

Toutes les versions de `Usermin` antérieures à la version 1.090.

3 Résumé

Deux vulnérabilités dans `Usermin` permettent à un utilisateur mal intentionné de porter atteinte à l'intégrité du système ou d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

`Usermin` est un outil d'administration pour les plates-formes Unix basé sur une interface web. Une première vulnérabilité concerne le script de création temporaire de répertoire `maketemp.pl` qui permet à un utilisateur mal intentionné de porter atteinte à l'intégrité du système (CAN-2004-0559).

Une seconde vulnérabilité concerne une mauvaise gestion des messages électroniques au format HTML permettant à un utilisateur mal intentionné d'exécuter de code malicieux, via un message électronique habilement constitué.

5 Solution

Mettre à jour Usermin en version 1.090.
Usermin est téléchargeable à l'adresse suivante :
<http://www.webmin.com/udownload.html>

6 Documentation

- Site Internet de Usermin :
<http://www.webmin.com/index6.html>
- Liste des changements dans Usermin :
<http://www.webmin.com/uchanges.html>
- Liste des changements dans Usermin version 1.090 :
<http://www.webmin.com/uchanges-1.090.html>
- Bulletin de sécurité SNS No.77 du 07 septembre 2004 :
http://www.lac.co.jp/security/csl/intelligence/SNSadvisory_e/77_e.html
- Bulletin de sécurité Gentoo GLSA 200409-15 du 12 septembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200409-15.xml>
- Bulletin de sécurité Debian DSA-544 du 14 septembre 2004 :
<http://www.debian.org/security/2004/dsa-544>
- Bulletin de sécurité Mandrake MDKSA-2004:101 du 22 septembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:101>
- Bulletin de sécurité FreeBSD pour webmin du 14 septembre 2004 :
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-0559 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0559>

Gestion détaillée du document

09 septembre 2004 version initiale.

13 septembre 2004 ajout de la référence au bulletin de sécurité de Gentoo.

14 septembre 2004 ajout de la référence au bulletin de sécurité de FreeBSD.

15 septembre 2004 ajout de la référence au bulletin de sécurité de Debian.

23 septembre 2004 ajout de la référence au bulletin de sécurité de Mandrake.