

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Webmin et 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-202>

Gestion du document

Référence	CERTA-2004-AVI-202-002
Titre	Vulnérabilité de Webmin et Usermin
Date de la première version	17 juin 2004
Date de la dernière version	28 juillet 2004
Source(s)	Bulletin de sécurité Gentoo GLSA 200406-12
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

- Déni de service ;
- divulgation d'informations confidentielles.

2 Systèmes affectés

- Webmin version 1.140-r1 et versions antérieures ;
- Usermin version 1.070 et versions antérieures ;

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans les outils Webmin et Usermin.

4 Description

Webmin et Usermin sont des outils d'administration pour les plates-formes Unix basé sur une interface web. Plusieurs vulnérabilités de Webmin et Usermin peuvent être exploitées par un utilisateur mal intentionné. La première vulnérabilité de Webmin permet à tous les utilisateurs d'avoir accès à la configuration des différents

modules, et d'obtenir ainsi des informations importantes sur le système.

La deuxième vulnérabilité concerne une mauvaise gestion par Usermin des messages électroniques au format HTML permettant l'exécution de code malicieux.

La troisième vulnérabilité concerne Webmin et Usermin. Un utilisateur mal intentionné peut, par le biais d'informations d'authentification erronées, bloquer l'accès du service aux utilisateurs légitimes.

5 Solution

- Mettre à jour l'outil Webmin. La version 1.150 corrige ces vulnérabilités.
- Mettre à jour l'outil Usermin. La version 1.080 corrige ces vulnérabilités.

6 Documentation

- Site Internet de Webmin et Usermin :
<http://www.webmin.com/>
- Site Internet des changements de Webmin :
<http://www.webmin.com/changes-1.150.html>
- Bulletin de sécurité SNS Advisory No. 74 du 11 juin 2004 :
http://www.lac.co.jp/security/csl/intelligence/SNSadvisory_e/74_e.html
- Bulletin de sécurité SNS Advisory No. 75 du 11 juin 2004 :
http://www.lac.co.jp/security/csl/intelligence/SNSadvisory_e/75_e.html
- Bulletin de sécurité Gentoo GLSA-200406-12 du 16 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-12.xml>
- Bulletin de sécurité Gentoo GLSA-200406-15 du 18 juin 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200406-15.xml>
- Bulletin de sécurité Debian DSA-526 du 03 juillet 2004 :
<http://www.debian.org/security/2004/dsa-526>
- Bulletin de sécurité Mandrake MDKSA-2004:074 du 27 juillet 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:074>
- Référence CVE CAN-2004-0582 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0582>
- Référence CVE CAN-2004-0583 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0583>

Gestion détaillée du document

17 juin 2004 version initiale.

05 juillet 2004 ajout des références à Usermin. Ajout des bulletins de sécurité SNS, Debian et des références CVE.

28 juillet 2004 ajout de la référence au bulletin de sécurité de Mandrake.