

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur wu-ftpd

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-2003-AVI-132>

Gestion du document

Référence	CERTA-2003-AVI-132-004
Titre	Vulnérabilité du serveur wu-ftpd
Date de la première version	01 août 2003
Date de la dernière version	4 septembre 2003
Source(s)	Avis SA:2003:032 de SuSE
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

Serveurs wu-ftpd versions 2.6.2 et antérieures.

3 Résumé

Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code avec les droits du super-utilisateur *root*.

4 Description

Le serveur wu-ftpd est un serveur ftp développé par l'université de Washington pour les plates-formes Unix.

Une vulnérabilité dans la gestion de la variable MAXPATHLEN permet d'exploiter un débordement de mémoire sur un seul octet ("*off-by-one*").

Pour exploiter cette vulnérabilité, l'utilisateur doit avoir un accès au serveur ftp, soit par un compte *anonymous*, soit par un compte utilisateur.

Certains noyaux Linux (versions 2.2.x et certaines anciennes versions 2.4.x) ne permettent pas d'exploiter cette vulnérabilité. En revanche, un serveur wu-ftp compilé avec un noyau 2.0.x ou 2.4.x récent (2.4.19 par exemple) est vulnérable.

5 Solution

Appliquer le correctif de votre éditeur.

6 Documentation

Avis de sécurité SA:2003:032 du SuSE :
http://www.suse.de/de/security/2003_032_wuftp.html

Avis de sécurité MDKSA-2003:080 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/>

Avis de sécurité de ISEC :
<http://isec.pl/vulnerabilities/isec-0011-wu-ftp.txt>

Avis de sécurité de Debian :
<http://www.debian.org/security/2003/dsa-357>

Avis de sécurité de RedHat :
– <http://rhn.redhat.com/errata/RHSA-2003-245.html>
– <http://rhn.redhat.com/errata/RHSA-2003-246.html>

Avis de sécurité SSRT3606 "Tru64 UNIX Internet Express wu-ftp Potential Security Vulnerability" de Hewlett-Packard :
<http://itrc.hp.com>

Avis de sécurité HPSBUX0309-277 "SSRT3603 wu-ftp off by one vulnerability" de Hewlett-Packard :
<http://itrc.hp.com>

Référence CVE CAN-2003-0466 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0466>

Gestion détaillée du document

01 août 2003 version initiale.

06 août 2003 première révision : correction de l'URL de l'avis ISEC.

18 août 2003 ajout références aux bulletins de sécurité de RedHat et Debian.

29 août 2003 ajout référence au bulletin de sécurité de Hewlett-Packard.

4 septembre 2003 ajout référence au bulletin de sécurité HPSBUX0309-277 de Hewlett-Packard pour HP-UX.