



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juillet 2004
N° CERTA-2004-AVI-074-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2004-AVI-074>

Gestion du document

Référence	CERTA-2004-AVI-074-003
Titre	Vulnérabilités du serveur wu-ftpd
Date de la première version	10 mars 2004
Date de la dernière version	17 juillet 2004
Source(s)	Bulletin de sécurité Debian DSA-457 du 08 mars 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

- Exécution de code arbitraire ;
- divulgation d'informations.

2 Systèmes affectés

wu-ftpd version 2.6.2.

3 Résumé

Deux vulnérabilités présentes sur le serveur wu-ftpd permettent à un utilisateur mal intentionné d'accéder à des informations confidentielles et d'exécuter du code arbitraire avec les privilèges du super utilisateur root.

4 Description

La première vulnérabilité concerne la restriction d'accès au répertoire d'un utilisateur : un utilisateur local mal intentionné peut en changeant les privilèges d'accès à son répertoire, accéder au répertoire racine du serveur wu-ftpd.

La seconde vulnérabilité concerne la méthode d'authentification skey : la non-vérification de la longueur de la variable name dans la fonction skey_challenge permet à un utilisateur mal intentionné distant d'exécuter du code arbitraire avec les privilèges du super utilisateur root.

5 Solution

Appliquer le correctif ou récupérer la mise à jour correspondant à votre système (cf. section documentation).

6 Documentation

- Bulletin de sécurité Debian DSA-457 du 08 mars 2004 :
<http://www.debian.org/security/2004/dsa-457>
- Bulletin de sécurité RedHat RHSA-2004:096 du 08 mars 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-096.html>
- Bulletin de sécurité FreeBSD du 08 mars 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité HPSBTU01012 pour HP Tru64 Unix du 08 avril 2004 :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01012>
- Bulletin de sécurité HPSBUX01059 pour HP-UX du 14 juillet 2004 :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01059>
- Référence CVE CAN-2004-0148 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0148>
- Référence CVE CAN-2004-0185 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0185>

Gestion détaillée du document

10 mars 2004 version initiale.

13 avril 2004 ajout référence au bulletin HPSBTU01012 pour HP Tru64 Unix.

13 mai 2004 ajout de la référence au bulletin de sécurité FreeBSD.

17 juillet 2004 modification des références aux bulletins de sécurité Debian et HP. Modification de la référence CVE CAN-2004-0148. Ajout de la référence au bulletin de sécurité HP-UX.