Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 juin 2000
N° CERTA-2000-ALE-010

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans le serveur de fichier wu-ftpd

Gestion du document

Référence	CERTA-2000-ALE-010
Titre	Vulnérabilités dans le serveur de fichier wu-ftpd
Date de la première version	26 juin 2000
Date de la dernière version	–
Source(s)	Avis Debian du 22 juin 2000 Serveur WEB du projet WU-FTP
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

- des utilisateurs locaux, distants ou anonymes peuvent usurper les privilèges du superutilisateur `root` sur la machine accueillant les serveurs ;
- des utilisateurs locaux, distants ou anonymes peuvent créer des répertoires et des fichiers dans le serveur ftp, permettant par exemple d'accueillir dans votre serveur ftp des sites au contenu au mieux illégitime au pire illégal ;
- des utilisateurs locaux, distants ou anonymes peuvent engendrer une charge de travail important sur le serveur, le rendant ainsi inapte à réaliser le service que l'on en attend.

Les risques sont actuellement très important dans la mesure où des programmes d'exploitation de certaines de ces vulnérabilités sont publiés.

2 Systèmes affectés

Les systèmes affectés par ces vulnérabilités sont les serveurs ftp `wu-ftpd` ou issus du code source de `wu-ftpd`.

3 Résumé

Certaines versions de `wu-ftp` sont vulnérables à une compromission à distance du compte `root` voire à une exploitation locale.

4 Description

`wu-ftpd` est un logiciel qui met en œuvre les services du *protocole de transfert de fichiers* (File Transfer Protocol ou FTP).

Depuis début 1999 un certain nombres de vulnérabilités ont été publiées sur ce logiciel ainsi que des programmes d'exploitation de ces vulnérabilités.

Certaines des compromissions décrites ci-après concernent non-seulement le logiciel `wu-ftpd` mais aussi les logiciels qui offrent le service ftp et qui sont basés sur le code source de `wu-ftpd`.

Les vulnérabilités sont les suivantes :

4.1 Débordement de pile dans MAPPING_CHDIR

Des utilisateurs distants et locaux peuvent exploiter cette vulnérabilité pour exécuter n'importe quel code avec les privilèges de l'utilisateur qui lance le serveur `wu-ftpd` (le plus souvent, le superutilisateur `root`).

Pour exploiter cette vulnérabilité, l'intrus doit être capable de créer des répertoires dans les systèmes vulnérables accessibles via FTP. Alors que les utilisateurs distants ne sont susceptibles d'avoir ce privilège qu'au travers d'un accès FTP anonyme, il se peut que les utilisateurs locaux aient la possibilité de créer les répertoires nécessaires dans leur répertoire personnel.

4.2 Débordement de pile dans le fichier message

Des utilisateurs distants et locaux peuvent exploiter cette vulnérabilité pour exécuter n'importe quel code avec les priviliège de l'utilisateur qui lance le serveur `wu-ftpd` (le plus souvent, le superutilisateur `root`).

Si les intrus sont capable de modifier le contenu d'un fichier `.message`, ils peuvent alors exploiter avec succès cette vulnérabilité. Cet accès est fréquemment accordé aux utilisateurs locaux dans leur répertoire personnel, mais il se peut que cette possibilité soit restreinte dans le cas de l'accès FTP anonyme, selon votre configuration.

En outre, dans certaines circonstances, il se peut que des utilisateurs distants soient capables de profiter de fichier `.message` contenant des macros fournis par l'administrateur du site en faisant en sorte que le client FTP fournissent des valeurs convenablement choisies qui seront exploitées par lesdites macros.

4.3 Fuite de mémoire dans SITE NEWER

Des intrus locaux ou distants qui peuvent se connecter au serveur FTP peuvent faire consommer une quantité de mémoire excessive, empêchant le fonctionnement normal du système. Si les intrus peuvent créer des fichiers sur le système, ils peuvent exploiter cette vulnérabilité pour exécuter n'importe quel code avec les privilège de l'utilisateur qui lance le serveur ftp, généralement le superutilisateur `root`.

4.4 Débordement de variable dans le programme *ftpshut*

Un débordement de variable est exploitable dans le programme `ftpshut` si celui est configuré avec les privilège `suid-root`. Ce peut utilisé par un utilisateur local pour obtenir un accès avec les privilège de `root`.

5 Solution

Des mises à jours de `wu-ftpd` sont fournies pour certaines distributions de systèmes d'exploitation. Il est souvent plus aisé pour la maintenance d'un site d'utiliser les mises à jours fournies par le vendeur plutôt que d'installer soit même à partir des sources. Cependant, on trouvera dans la section 5.1 des avertissement sur certains aspects de la configuration qu'on ne retrouve pas dans les autres sections.

Si votre distribution n'est pas citée reportez vous à la section 5.1.

5.1 Correction manuelle

Charger la dernière version des sources du logiciel `wu-ftpd` à l'adresse
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.0.tar.gz .
Appliquez le correctif suivant aux sources :
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/quickfixes/apply_to_2.6.0/lreply-buffer-overflow.patch .
Il faut maintenant configurer le serveur avant de le compiler.

Attention ! il se peut que la version 2.6.0 pose des problèmes d'interopérabilité avec certains clients FTP bogués. En effet, la version 2.6.0 a été corrigée pour accroître sa conformité à la RFC spécifiant le protocole FTP. En conséquence il se peut que certains clients qui ne respectent pas totalement la RFC cesse d'interopérer avec le serveur. Nous vous encourageons à bien lire la documentation de `wu-ftp` avant de faire la mise à jour.

Si la compatibilité de votre serveur avec des logiciels clients non conformes à la RFC est un soucis pour le service FTP que vous rendez, il y a lieu de configurer avec les options suivantes :

```
./configure --enable-badclients
```

Il se peut que dans des versions futures de `wu-ftpd` cette option de configuration ne soit plus disponible.
Compilez et installez.
Par défaut `ftpshut` n'est pas installé avec les privilège `suid-root`.
Il peut s'avérer nécessaire de prendre les mesures suivantes :

- désactiver ou limiter les zones du serveur où on l'on peut déposer des fichiers.
  De nombreux sites offre le service FTP à une communauté. Par exemple, une communauté de développeur de logiciels libres peut mettre en place un serveur FTP ou chacun peut déposer ses logiciels dans un répertoire (généralement appelé `Incomming`). Ce répertoire, quoique peu sûr, permet une gestion souple du serveur qui se conçoit dans une communauté informelle.
  Une telle approche peut permettre à des intrus d'abuser du service offert en offrant des fichiers qui ne sont pas dans l'esprit que vous souhaitez donner à votre site. Par exemple, un intrus pourrait, à votre insu, créer chez vous un serveur de fichiers au caractère douteux qui :

  1° consomme à vos frais des ressources.
  Les intrus occupent en général les serveurs FTP d'autrui pour y placer des fichiers que l'on trouve difficilement mais qui pour autant peuvent être très demandés. Un fort volume de fichiers déposés dans votre serveur se fera au détriment de la place que vous pourrez accorder aux fichiers pour lesquels vous avez monté votre service FTP. Par ailleurs, une forte demande peut engendrer une forte charge sur vos serveurs au point qu'ils ne rendent pas le service pour lequel ils ont été créés avec la diligence nécessaire.

  2° pose un problème d'image.
  Votre organisme n'aurait peut-être pas publié ou toléré la publication de fichiers tels que ceux qu'a déposé l'intrus. Par exemple, il est peu probable qu'une administration publie des documents qui incitent à la haine, ou qu'un site prônant la francophonie soit inondés de textes dans une langue étrangère.

  3° engage votre responsabilité.
  On constate de plus en plus la réaction violente des éditeurs de logiciel, de musique voire d'œuvres littéraires face à ce qu'ils considèrent comme du pillage. Il arrive moins souvent que des artistes ou des particuliers réagisse ainsi lorsqu'ils estiment bafoués leur droit (relatif à leur image par exemple). Indépendemment du bien fondé de leur démarche dans le cas précis des fichiers qui pourraient être placés à votre insu sur vos serveurs de fichiers, il se peut que vous fassiez l'objet d'une plainte.

Configurez par conséquent votre serveur FTP pour limiter la possibilité de déposer des fichiers au minimum nécessaire pour rendre le service que vous souhaitez. Une documentation en anglais est disponible sur à l'adresse :
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/upload.configuration.HOWTO

5.2 Debian

5.2.1 Debian 2.1 (slink)

Source

- http://security.debian.org/dists/slink/updates/source/wu-ftpd-academ_2.4.2.16-13.1.diff.gz

- http://security.debian.org/dists/slink/updates/source/wu-ftpd-academ_2.4.2.16-13.1.dsc
- http://security.debian.org/dists/slink/updates/source/wu-ftpd-academ_2.4.2.16.orig.tar.gz

alpha http://security.debian.org/dists/slink/updates/binary-alpha/wu-ftpd-academ_2.4.2.16-13.1_alpha.deb
i386 http://security.debian.org/dists/slink/updates/binary-i386/wu-ftpd-academ_2.4.2.16-13.1_i386.deb
m68k http://security.debian.org/dists/slink/updates/binary-m68k/wu-ftpd-academ_2.4.2.16-13.1_m68k.deb
sparc http://security.debian.org/dists/slink/updates/binary-sparc/wu-ftpd-academ_2.4.2.16-13.1_sparc.deb

5.2.2 Debian 2.2 (potato)

Source

- http://security.debian.org/dists/potato/updates/main/source/wu-ftpd_2.6.0-5.1.diff.gz
- http://security.debian.org/dists/potato/updates/main/source/wu-ftpd_2.6.0-5.1.dsc
- http://security.debian.org/dists/slink/updates/source/wu-ftpd-academ_2.4.2.16.orig.tar.gz

alpha http://security.debian.org/dists/potato/updates/main/binary-alpha/wu-ftpd_2.6.0-5.1_alpha.deb
arm http://security.debian.org/dists/potato/updates/main/binary-arm/wu-ftpd_2.6.0-5.1_arm.deb
i386 http://security.debian.org/dists/potato/updates/main/binary-i386/wu-ftpd_2.6.0-5.1_i386.deb
m68k http://security.debian.org/dists/potato/updates/main/binary-m68k/wu-ftpd_2.6.0-5.1_m68k.deb
powerpc http://security.debian.org/dists/potato/updates/main/binary-powerpc/wu-ftpd_2.6.0-5.1_powerpc.deb
sparc http://security.debian.org/dists/potato/updates/main/binary-sparc/wu-ftpd_2.6.0-5.1_sparc.deb

5.3 Redhat linux

Installez les extensions au travers des fichiers `rpm` suivants (pour chaque fichier `rpm` correspondant à votre architecture matérielle, lancez : `rpm -Fvh [fichier]` où *fichier* est le nom du fichier `rpm`) :

5.3.1 Red Hat Linux 5.2

i386 ftp://updates.redhat.com/5.2/i386/wu-ftpd-2.6.0-2.5.x.i386.rpm
alpha ftp://updates.redhat.com/5.2/alpha/wu-ftpd-2.6.0-2.5.x.alpha.rpm
sparc ftp://updates.redhat.com/5.2/sparc/wu-ftpd-2.6.0-2.5.x.sparc.rpm
sources ftp://updates.redhat.com/5.2/SRPMS/wu-ftpd-2.6.0-2.5.x.src.rpm

5.3.2 Red Hat Linux 6.2

i386 ftp://updates.redhat.com/6.2/i386/wu-ftpd-2.6.0-14.6x.i386.rpm
alpha ftp://updates.redhat.com/6.2/alpha/wu-ftpd-2.6.0-14.6x.alpha.rpm
sparc ftp://updates.redhat.com/6.2/sparc/wu-ftpd-2.6.0-14.6x.sparc.rpm
sources ftp://updates.redhat.com/6.2/SRPMS/wu-ftpd-2.6.0-14.6x.src.rpm

6 Documentation

De plus amples informations sur les sites :

- http://www.debian.security/2000/20000623 ;
- http://www.redhat.com/support/errata/RHSA-2000-039-02.html ;
- http://www/wu-ftpd.org .

Gestion détaillée du document

26 juin 2000 version initiale.