Projet Fuzzer

Maël Delorme, Geoffrey Lacotte, Nishith Puranik, Jean-Philippe Monjot

2022-2023

Table des matières

1 Introduction

Ce rapport présente notre projet fuzzer pour les deux serveurs FTP cibles, à savoir Pure-FTPd et LightFTP.

1.1 Synthèse

Pour résumer ce qui a été réalisé, ce projet permet d'envoyer des commandes aléatoires générées grâce à de la grammaire dharma sur le compte Anonymous de Pure-FTPd.
Nous n'avons malheureusement pas réussi à tester concrètement LightFTP avec notre programme.

2 Installation

Pour expliquer au mieux comment nous avons préparé notre environnement de test, nous allons détailler ici l'installation des serveurs FTP depuis une machine Virtuelle Debian 11 fraîchement installée pour chaque serveur.
Nous utilisons le dépôt publique de notre projet sur github afin d'effectuer l'entièreté de l'installation via un shell.

2.1 Pure-FTPd

2.1.1 Installation des paquets nécessaires

sur la console :

```
apt-get install build-essential
apt-get install python3
apt-get install pip
apt-get install git
apt-get install ftp
pip install dharma
apt-get install Pure-FTPd
```

2.1.2 Configuration de Pure-FTPd

L'idée est de permettre un accès anonyme à Pure-FTPd afin de lancer des commandes. Ainsi nous suivons le tutoriel suivant : `https://fuzzysecurity.com/tutorials/1.html`. Voici les commandes que nous avons tapées en tant que root :

```
groupadd ftpgroup
useradd -g ftpgroup -d /dev/null -s /etc ftpuser
mkdir /root/ftphome
pure-pw useradd ftp -u ftpuser -g ftpgroup -d /root/ftphome/
mot de passe : pass
pure-pw mkdb
ln -s /etc/pure-ftpd/pureftpd.passwd /etc/pureftpd.passwd
ln -s /etc/pure-ftpd/pureftpd.pdb /etc/pureftpd.pdb
ln -s /etc/pure-ftpd/conf/PureDB /etc/pure-ftpd/auth/PureDB
chown -R ftpuser:ftpgroup /root/ftphome
/etc/init.d/pure-ftpd restart
```

Nous modifions aussi le fichier */etc/pure-ftpd.conf*, de manière à permettre les accès anonymous, c'est-à-dire que nous faisons passer l'option *NoAnonymous* yes à no.
De même dans le fichier : */etc/pure-ftpd/conf/NoAnonymous*.
Sans oublier de relancer le Pure-FTPd par la suite : /etc/init.d/pure-ftpd restart

Si en lançant le programme vous avez une erreur 421, il suffit d'exécuter les commandes suivantes :

```
mkdir /var/ftp
chown ftpuser:ftpgroup /var/ftp
usermod ftp -d /var/ftp
useradd -d /var/ftp -s /sbin/nologin ftpE
```

2.2 LightFTP

Sur la console :

```
apt-get install build-essential
apt-get install python3
```

```
apt-get install pip
apt-get install ftp
pip install dharma
apt-get install git
apt install gnutls-dev

git clone https://github.com/hfiref0x/LightFTP.git
cd /LightFTP/Source/Release/
make

mkdir /root/fftp/
mkdir /root/ftpshare/
touch /root/fftp/log

cd ~/LightFTP/Bin/
nano fftp.conf

changement des lignes suivantes :
logfilepath=/root/fftp/log

[anonymous]
root=/root/ftpshare

[uploader]
root=/root/ftpshare

[webadmin]
root=/root/ftpshare
```

Si l'erreur suivante apparaît : *"Failed to start server. Can not bind to address"*. Essayez de changer le port dans le fichier de configuration *fttp.conf*.

Exécution de LightFTP :
Dans le dossier /LightFTP/Source/Release : *./fftp ../../Bin/fttp.confd*

Pour se connecter en shell : ftp 127.0.0.1

2.3 Installation de notre projet

Placez-vous dans un dossier (par exemple le home), et exécutez la commande : *git clone https ://github.com/Iluvrog/fuzzing.git.*
Ou bien décompressez l'archive fournie avec ce rapport.

2.4 Exécution de notre programme

Pour exécuter notre programme, il suffit d'aller dans le dossier fuzzing, et d'exécuter la commande suivante : *python3 main.py.*

Si le programme s'exécute sans commentaire, c'est qu'il a réussi à se connecter sur le serveur FTP et à exécuter les commandes générées aléatoirement.

3 Description/Configuration de notre programme

Une description de notre programme peut être retrouvée dans le fichier readme du dépôt github.

Nous utilisons la librairie ftplib de python pour établir une connexion ftp, par défaut il s'agit du compte anonymous sur l'adresse localhost et sur le port 21.
Vous pouvez modifier cela dans le fichier /src/ftp.py dans les paramètres de la fonction connexion.

Le résultat de l'exécution du programme se trouve dans le dossier *resultats* avec comme fichier :
- *resultat_dharma_test.txt* où sont écrites les commandes générées aléatoirement par dharma.
- *error.txt* où sont écrites les erreurs obtenues, c'est-à-dire quand la connexion n'est pas établie, ou quand une commande lève une exception.

4 Test

Nous n'avons malheureusement pas eu la motivation d'exécuter des tests autres que le bon fonctionnement de notre code.
Voici un exemple de sortie de notre programme :
- fichier error.txt :

```
19/05/2023 11:40:19 :
Commande : nlist , resultat : 500 Unknown command


19/05/2023 11:40:19 :
Commande : struct /k9u9w9z/, resultat : 500 Unknown command


19/05/2023 11:40:19 :
Commande : ls , resultat : 500 Unknown command


19/05/2023 11:40:19 :
Commande : delete 9, resultat : 500 HTTP command: [delete]


19/05/2023 11:40:19 :
Commande : chmod a/69/w0nsw.mp3, resultat : [Errno 104] Connection reset by peer
```

Puis, pour pour le fichier *resultat_dharma_test.txt* :

```
Liste des commandes generees :
- nlist
- struct /k9u9w9z/
- ls
- delete 9
- chmod a/69/w0nsw.mp3
```

Durant nos tests, nous obtenons en majorité des erreurs 500 ou des erreurs de type *broken pipe*.

5 Amélioration

Le premier test que nous aurions voulu faire est la CVE-2020-35359 comme indiqué ici : sous-section 6.4, car l'exploit est déjà fourni.

La deuxième aurait été la CVE-2023-24042 comme indiqué ici : sous-sous-section 6.1.1, car cette vulnérabilité a été trouvée grâce à des requêtes malformées.

Ensuite, proposer une solution plus user-friendly pour permettre de changer l'utilisateur, l'adresse et le port plus facilement.

6 Recherche de l'existant pour les vulnérabilités de LightFTP et Pure-FTPd

6.1 LightFTP

6.1.1 CVE-2023-24042

Dans la release 2.3 de LightFTP, nous voyons qu'il s'agit principalement d'une correction d'un bug qui permettait de faire du path traversal.
Plus précisément, la base de données du NIST indique qu'il s'agit d'une condition de concurrence depuis LightFTP 2.2 via une requête malformée, typiquement une vulnérabilité qui peut être trouvée par un fuzzer.

Le détail de cette CVE peut être retrouvé sur le projet github ici :
`https://github.com/hfiref0x/LightFTP/issues/25`

6.1.2 CVE-2017-1000218

En recherchant dans la base de données du NIST, nous voyons une autre vulnérabilité liée à LightFTP, Il s'agit cette fois d'un buffer overflow dans la version 1.1 du logiciel.

Le détail de cette CVE peut être retrouvé sur le projet github ici :
`https://github.com/hfiref0x/LightFTP/issues/5`

6.2 Pure-FTPd

Sur cvedetails.com nous pouvons retrouver 9 vulnérabilités pour Pure-FTPd.

6.3 CVE-2021-40524

Dans les versions entre 1.0.23 et 1.0.49 de Pure-FTPd, une vérification de la taille d'un fichier à téléverser a pu être contournée, entraînant ainsi le téléversement de taille conséquente pouvant amener à un déni de service.

Le détail de cette CVE peut être retrouvé sur le projet github ici :
`https://github.com/jedisct1/pure-ftpd/pull/158`

6.4 CVE-2020-35359

Dans la version 1.0.48 de Pure-FTPd, un attaquant distant peut empêcher l'utilisation légitime du serveur en établissant suffisamment de connexions pour dépasser la limite du nombre de session établie.
Cette vulnérabilité pourrait être trouvée par un fuzzer en établissant suffisamment de connexions.

L'exploitation de cette CVE peut être trouvée ici :
`https://www.exploit-db.com/exploits/49105`

6.5 CVE-2020-9365

Cette vulnérabilité a été trouvée lors de la version 1.0.49 de Pure-FTPd, elle permet à un attaquant d'aller lire dans une zone mémoire non prévue à cet effet.

La correction de cette vulnérabilité peut être trouvée ici : `https://github.com/jedisct1/pure-ftpd/commit/bf6fcd4935e95128cf22af5924cdc8fe5c0579da`

6.6 CVE-2020-9274

Cette vulnérabilité a été trouvée lors de la version 1.0.49 de Pure-FTPd, Il s'agit d'un pointeur non initialisé dans la liste chaînées *diraliases*.

La correction de cette vulnérabilité peut être trouvée ici : `https://github.com/jedisct1/pure-ftpd/commit/8d0d42542e2cb7a56d645fbe4d0ef436e38bcefa`

6.7 CVE-2019-20176

Dans Pure-FTPd 1.0.49, un problème d'épuisement de la pile a été découvert dans la fonction listdir, pouvant mener à un déni de service.

La correction de cette vulnérabilité peut être trouvée ici : `https://github.com/jedisct1/pure-ftpd/commit/aea56f4bcb9948d456f3fae4d044fd3fa2e19706`

6.8 CVE-2017-12170

La version 1.0.46-1 en aval de Pure-FTPd telle que livrée dans Fedora était vulnérable à une erreur d'empaquetage dans laquelle la configuration d'origine a été ignorée après la mise à jour et le service commençait à fonctionner avec la configuration par défaut.

6.9 CVE-2011-1575

L'implémentation de STARTTLS dans ftp_parser.c dans Pure-FTPd avant la version 1.0.30 ne limite pas correctement la mise en mémoire tampon des E/S, ce qui permet aux attaquants de faire une attaque de type MITM et d'insérer des commandes dans des sessions FTP chiffrées en envoyant une commande en texte clair qui est traitée après la session TLS soit établie.

La correction de cette vulnérabilité peut être trouvée ici : `https://github.com/jedisct1/pure-ftpd/commit/65c4d4ad331e94661de763e9b5304d28698999c4`

6.10 CVE-2011-0988

Dans la version 1.0.22 de Pure-FTPd et plus précisément sur SUSE, Enterprise Server/Desktop 10 SP3 et SP4, lors de l'exécution des extensions OES Netware, il était possible de créer un répertoire accessible en écriture par tous, qui permettait aux utilisateurs locaux d'écraser des fichiers arbitraires et de faire des escalation de privilège via des vecteurs non spécifiés.

Un billet de sécurité sur IBM X-Force Exchange peut être trouvé ici :
`https://exchange.xforce.ibmcloud.com/vulnerabilities/66618`

6.11 CVE-2011-0418

L'implémentation de glob dans les versions inférieures à 1.0.32, et dans libc sous NetBSD 5.1, ne développe pas correctement les expressions contenant des accolades, ce qui permet aux utilisateurs distants authentifiés de provoquer un déni de service via une commande FTP STAT spécialement construite.