Invasion OpenWrt sur Xiaomi Mi Router 4C

C’est ma troisième tentative d’installer OpenWrt. La première fois, c’était en 2019, lorsque j’ai utilisé un port UART pour me connecter. La deuxième fois, en 2023, j’ai utilisé une méthode similaire à celle décrite ici.

Le code d’exploitation peut être trouvé à https://github.com/acecilia/OpenWRTInvasion.

Tout d’abord, installez les exigences :

```
pip install -r requirements.txt --break-system-packages
```

Après avoir exécuté l’exploitation, vous pouvez accéder à l’interface web du routeur à une URL similaire à celle-ci (la valeur `stok` variera) :

```
http://192.168.1.28/cgi-bin/luci/;stok=fe9b14c5c4dee48709fbdf00e048d5ec/web/home
```

“bash lzwjava@anonymous OpenWRTInvasion % python remote_command_execution_vulnerability.py Adresse IP du routeur [appuyez sur Entrée pour utiliser la valeur par défaut 'miwifi.com']: 192.168.1.28 Entrez le mot de passe de l'administrateur du routeur: ... Il y a deux options pour fournir les fichiers nécessaires à l'invasion : 1. Utiliser un serveur de fichiers TCP local fonctionnant sur un port aléatoire pour fournir des fichiers dans le répertoire localscript_tools‘. 2. Télécharger les fichiers nécessaires à partir du dépôt GitHub distant. (choisissez cette option uniquement si GitHub est accessible à partir de l’appareil routeur.) Quelle option préférez-vous ? (par défaut : 1)1 ********** adresse_ip_du_routeur: 192.168.1.28 stok: 08f4f22fed20b94580cb8e70703c941c fournisseur_de_fichiers: serveur de fichiers local ********** début du téléchargement du fichier de configuration…début de l’exécution de la commande…le serveur de fichiers local fonctionne sur 0.0.0.0:63067. root=‘script_tools’ le serveur de fichiers local obtient ‘busybox-mipsel’pour 192.168.1.28. le serveur de fichiers local obtient ‘dropbearStaticMipsel.tar.bz2’pour 192.168.1.28. terminé ! Vous pouvez maintenant vous connecter au routeur via plusieurs options : (utilisateur : root, mot de passe : root) * telnet 192.168.1.28 * ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c 3des-cbc -o UserKnownHostsFile=/dev/null root@192.168.1.28 * ftp : en utilisant un programme comme Cyberduck

root@XiaoQiang:/tmp# wget “https://downloads.openwrt.org/releases/24.10.0/targets/ramips/mt76x8/openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin”wget: pas une URL http ou ftp: https://downloads.openwrt.org/releases/24.10.0/targets/ramips/mt76x8/openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin

scp -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c 3des-cbc openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin root@192.168.1.28:/tmp/ ash: /usr/libexec/sftp-server: introuvable scp: Connexion fermée

cat openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin | ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa root@192.168.1.28 “cat > /tmp/openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin”

root@XiaoQiang:/tmp# ls 2541.bootcheck.log oui TZ rc.done appStoreRule.json rc.timing arrays resolv.conf authenfailed-cache resolv.conf.auto busybox root daemon rr datalist run dropbear script.sh dropbear.tar.bz2 speedtest_urls.xml etc spool ftpd startscene_crontab.lua.PID lock stat_points_privacy.log log stat_points_rom.log logexec state luci-indexcache sysapihttpd luci-nonce sysapihttpdconf luci-sessions sysinfo messages syslog-ng.ctl miqos.lock syslog-ng.pid mnt taskmonitor mt76xx2.sh.log uci2dat_mt7628.log network.env uploadfiles nginx_check.log upnp.leases ntp.status web_config_list openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin wifi_analysis.log

root@XiaoQiang:/tmp# mtd -r write openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin OS1 Déverrouillage de OS1 …

Écriture de openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin vers OS1 …[w]

Connectez-vous au routeur via une connexion filaire. Vous pouvez ensuite accéder à l’interface web à 192.168.1.1 ou utiliser SSH en exécutant `ssh root@192.168.1.1`.