OpenWrt Invasion auf Xiaomi Mi Router 4C

Dies ist mein dritter Versuch, OpenWrt zu installieren. Das erste Mal war 2019, als ich einen UART-Port zum Verbinden verwendet habe. Das zweite Mal war 2023, als ich eine ähnliche Fernmethode wie die hier beschriebene verwendet habe.

Der Exploit-Code kann unter https://github.com/acecilia/OpenWRTInvasion gefunden werden.

Zuerst installieren Sie die Anforderungen:

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

Nach dem Ausführen des Exploits können Sie auf die Weboberfläche des Routers über eine URL ähnlich dieser zugreifen (der `stok`-Wert wird variieren):

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

“bash lzwjava@anonymous OpenWRTInvasion % python remote_command_execution_vulnerability.py Router IP-Adresse [Drücken Sie die Eingabetaste, um die Standardadresse 'miwifi.com' zu verwenden]: 192.168.1.28 Geben Sie das Admin-Passwort des Routers ein: ... Es gibt zwei Optionen, um die für die Invasion benötigten Dateien bereitzustellen: 1. Verwenden Sie einen lokalen TCP-Dateiserver, der auf einem zufälligen Port läuft, um Dateien im lokalen Verzeichnisscript_tools‘ bereitzustellen. 2. Laden Sie die benötigten Dateien von einem entfernten GitHub-Repository herunter. (Wählen Sie diese Option nur, wenn GitHub innerhalb des Router-Geräts zugänglich ist.) Welche Option bevorzugen Sie? (Standard: 1)1 ********** router_ip_address: 192.168.1.28 stok: 08f4f22fed20b94580cb8e70703c941c file provider: lokaler Dateiserver ********** Starten des Hochladens der Konfigurationsdatei...Starten des Befehlsausführungsbefehls...Lokaler Dateiserver läuft auf 0.0.0.0:63067. root=‘script_tools’Lokaler Dateiserver stellt ‘busybox-mipsel’für 192.168.1.28 bereit. Lokaler Dateiserver stellt ‘dropbearStaticMipsel.tar.bz2’für 192.168.1.28 bereit. Fertig! Jetzt können Sie sich mit dem Router über mehrere Optionen verbinden: (Benutzer: root, Passwort: 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: Verwenden Sie ein Programm wie 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-sysupgr ade.bin”wget: keine http- oder ftp-URL: 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: nicht gefunden scp: Verbindung geschlossen

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 OS1 wird entsperrt …

Schreiben von openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin in OS1 …[w]

Verbinden Sie sich über eine kabelgebundene Verbindung mit dem Router. Sie können dann auf die Weboberfläche unter 192.168.1.1 zugreifen oder SSH verwenden, indem Sie `ssh root@192.168.1.1` ausführen.