

開源路由器入侵小米路由器 4C

這是我第三次嘗試安裝 OpenWrt。第一次是在 2019 年，當時我使用 UART 端口連接。第二次是在 2023 年，我使用了一種與這裡描述相似的遠程方法。

漏洞代碼可以在 <https://github.com/acecia/OpenWRTInvasion> 找到。

首先，安裝所需項目：

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

運行漏洞代碼後，您可以通過類似以下的 URL 訪問路由器的網頁介面（stok 值會有所不同）：

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

```
lzwjava@anonymous OpenWRTInvasion % python remote_command_execution_vulnerability.py
```

```
Router IP address [press enter for using the default 'miwifi.com']: 192.168.1.28
```

```
Enter router admin password: ...
```

There two options to provide the files needed for invasion:

1. Use a local TCP file server running on random port to provide files in local directory `script_tools`.
2. Download needed files from remote github repository. (choose this option only if github is accessible in the environment)

Which option do you prefer? (default: 1)1

```
router_ip_address: 192.168.1.28
```

stok: 08f4f22fed20b94580cb8e70703c941c

```
file provider: local file server
```

```
start uploading config file...
```

```
start exec command...
```

```
local file server is runing on 0.0.0.0:63067. root='script_tools'
```

```
local file server is getting 'busybox-mipsel' for 192.168.1.28.
```

```
local file server is getting 'dropbearStaticMipsel.tar.bz2' for 192.168.1.28.
```

done! Now you can connect to the router using several options: (user: root, password: root)

```
* telnet 192.168.1.28
```

```
* ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c 3des-cbc -o UserKnownHostsF
```

- * ftp: using a program like cyberduck

```
root@XiaoQiang:/tmp# wget "https://downloads.openwrt.org/releases/24.10.0/targets/ramips/mt76x8/openwrt-24.10.0-rc2-ramips-mt76x8-generic-squashfs-kernel.bin"
ade.bin"
```

```
wget: not an http or ftp url: https://downloads.openwrt.org/releases/24.10.0/targets/ramips/mt76x8/openwrt-24
```

```
scp -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -c 3des-cbc openwrt-24.10.0-ramdisk
```

```
ash: /usr/libexec/sftp-server: not found
```

```
scp: Connection closed
```

```
cat openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin | ssh -oKexAlgorithms=+diffie-h
```

```
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 0
```

```
Unlocking OS1 ...
```

```
Writing from openwrt-24.10.0-ramips-mt76x8-xiaomi_mi-router-4c-squashfs-sysupgrade.bin to OS1 ... [w]
```

通過有線連接連接路由器。然後，您可以通過 192.168.1.1 訪問網頁介面，或者通過運行 `ssh root@192.168.1.1` 使用 SSH。