INSOMNIA

SECURITY SPECIALISTS :: REST SECURED

Router Hacking

CHCon 2018

Router Hacking

$ whoami

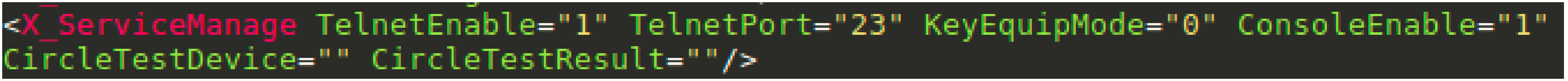
- Ben `[zante]` 🐦 @zantedotnz
- Security Consultant @ Insomnia Security
- Previously, Digital Forensic Analyst @ NZ Police
- Interested in hacking embedded devices. Pulling flash chips off. Finding crazy command injection bugs.

Motivation

- Huawei HG659 for iptables access to redirect DNS for US Netflix goodness
- Find vulnerabilities in current generation routers
- Learn about hardware hacking

Huawei HG659

- Well researched, decrypt/encrypt the configuration backup XML to enable telnet and recover root password



```
<X_ServiceManage TelnetEnable="1" TelnetPort="23" KeyEquipMode="0" ConsoleEnable="1"
CircleTestDevice="" CircleTestResult=""/>
```

- Original research: https://hg658c.wordpress.com

New Research

- Command injection vulnerabilities in three routers:
  - Huawei B618
  - Huawei B315
  - [REDACTED]
- Exploitation requires either web admin or physical access

[REDACTED]? 😟

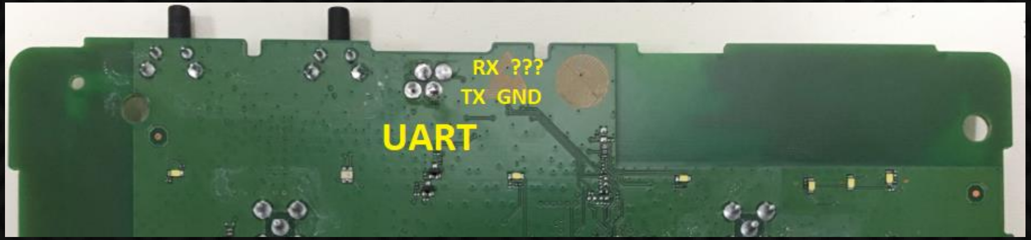
- Vendor told their customer the vulnerability had been patched … it wasn’t though, so it’s still unpatched
- Interesting bug I really want to share
- Keep an eye on Twitter and I’ll post the vulnerability report when I can do so publicly

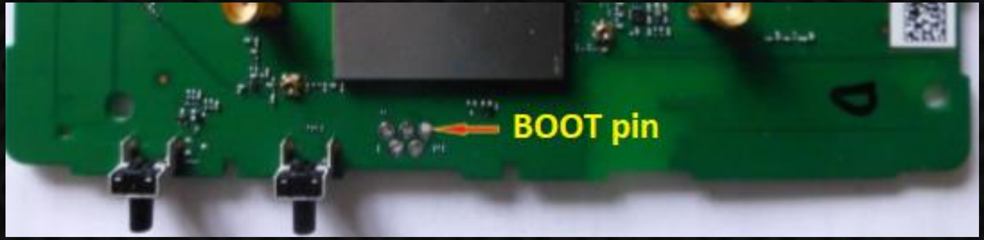
Vulnerability Disclosure

- I just want to talk about the bugs but it’s more complicated than that
- Give yourself a long lead time if you want to talk about vulnerabilities publicly
- If you’re unknown to an organisation, disclose through a trusted third-party
- If you receive vulnerability reports, be kind
- If you send vulnerability reports, be respective

Hardware Hacking

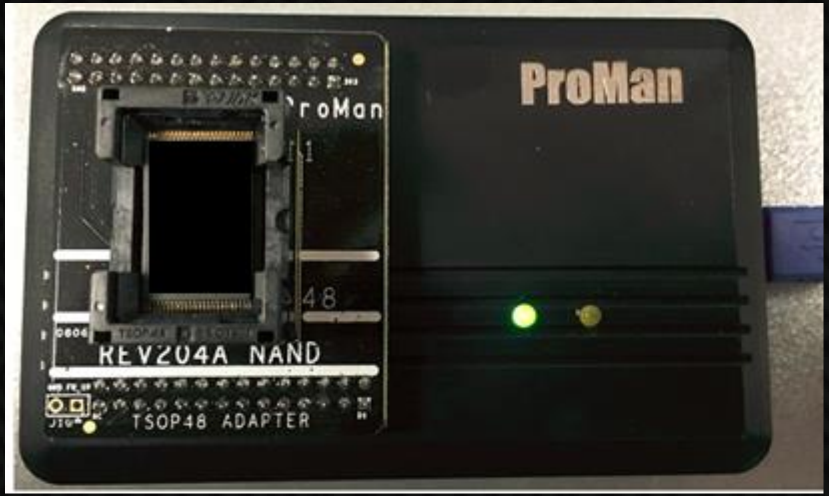
- Used to assist with vulnerability discovery
- UART for debug messages
- BOOT PIN for Huawei firmware reflashing without signature verification





Hardware Hacking

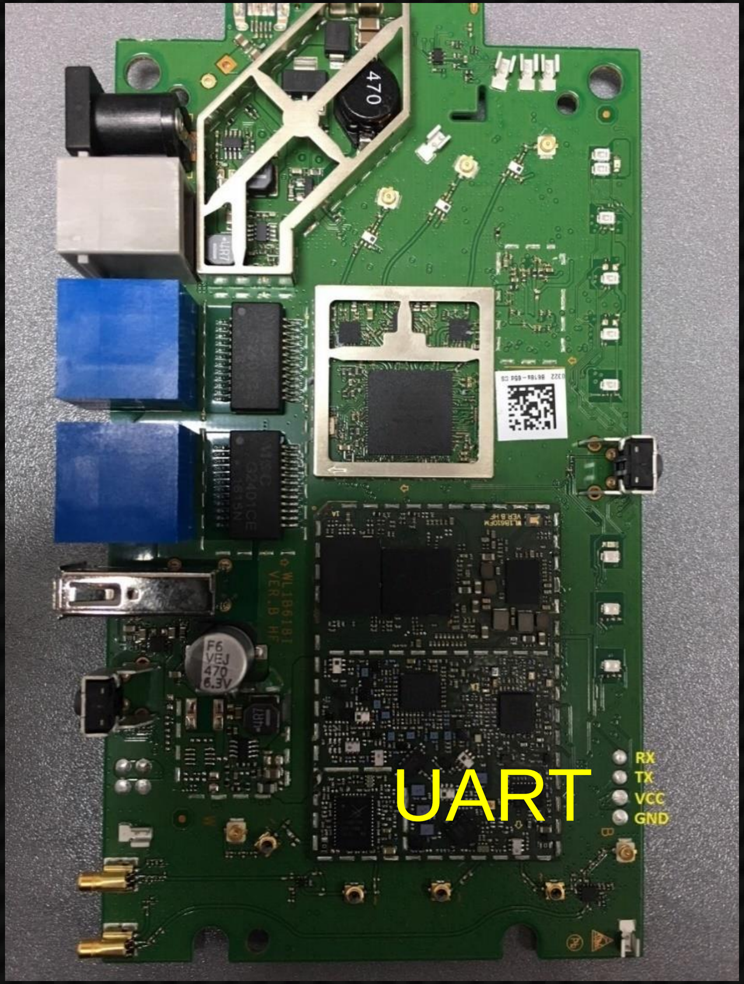
- Chip-Off for firmware dump (encrypted firmware image)
- Huawei B618 uses an non-standard sized BGA flash chip

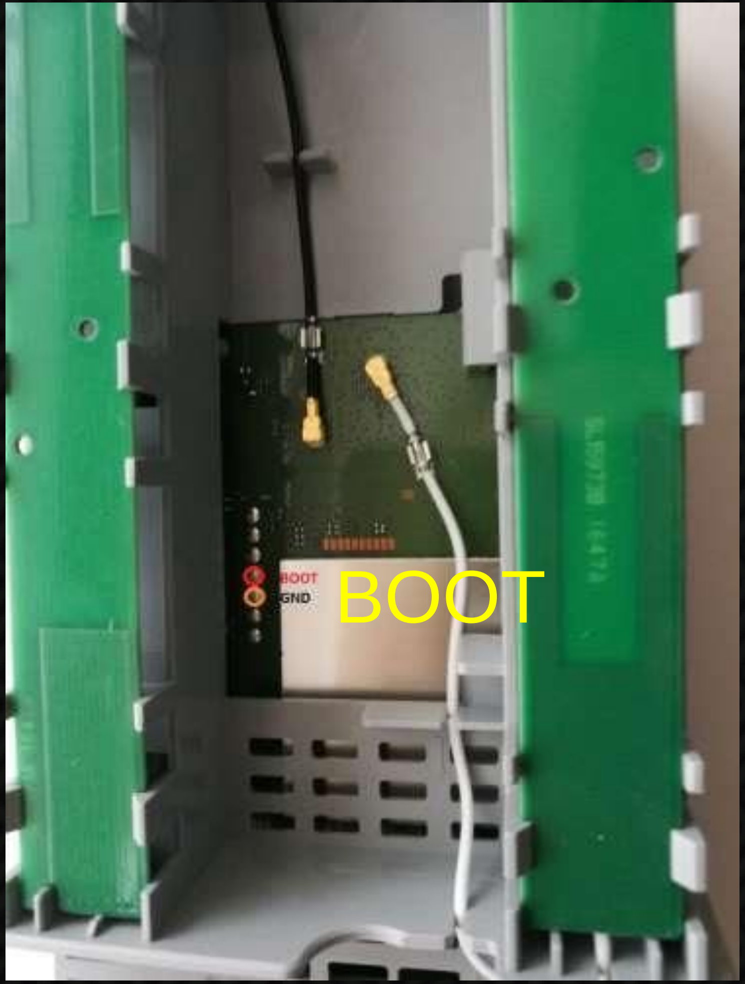


Research Methodology

- Remove the casing and review the hardware
- Connect to UART, JTAG and any other debug ports
- Grab the firmware (download or chip-off dump)
- Enable all the services (SMB, DLNA, VPN, etc)
- Look for the low-hanging fruit vulnerabilities
- Functionality that gives you some feedback of success
- Monitor process execution, networking and file system events (strace, fsmon or UART)

Huawei B618





root@p750:/etc/ppp/peers # cat vpn1234

```
# written by pptpsetup
plugin "pptp.so"
name vpn1234
pptp_server 10.1.1.1
file /etc/ppp/options.pptp
noauth
nobsdcomp
nodeflate
name zante
plugin /online/firmware1.bin
```

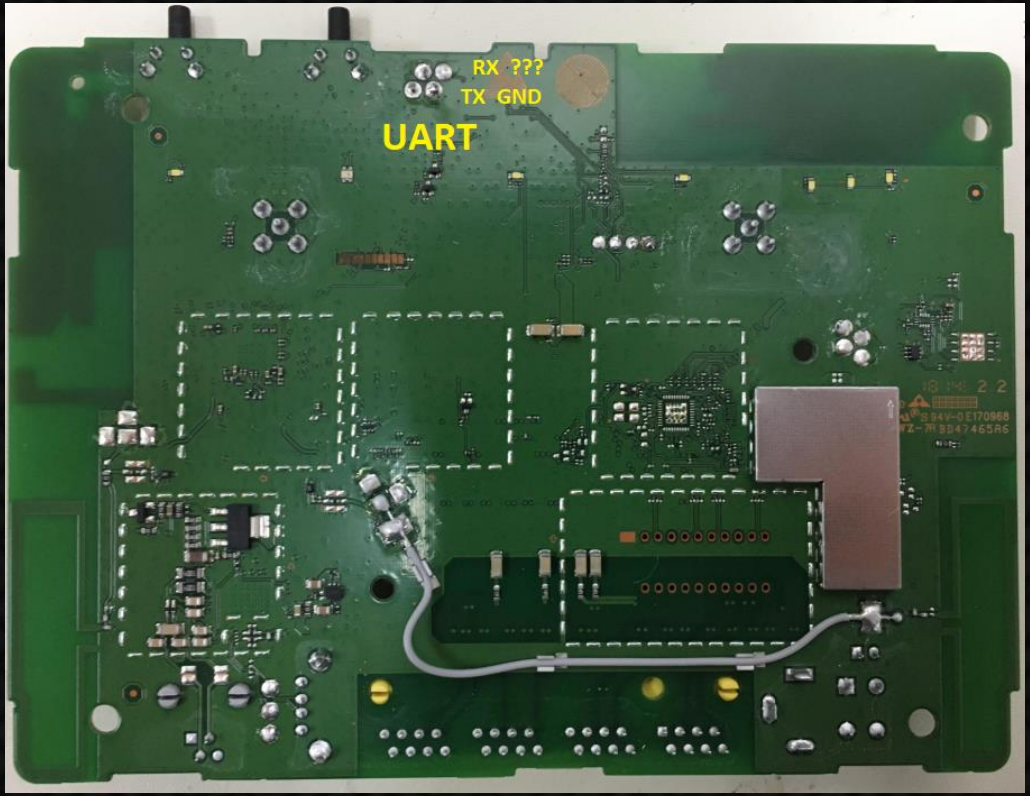
new line injection

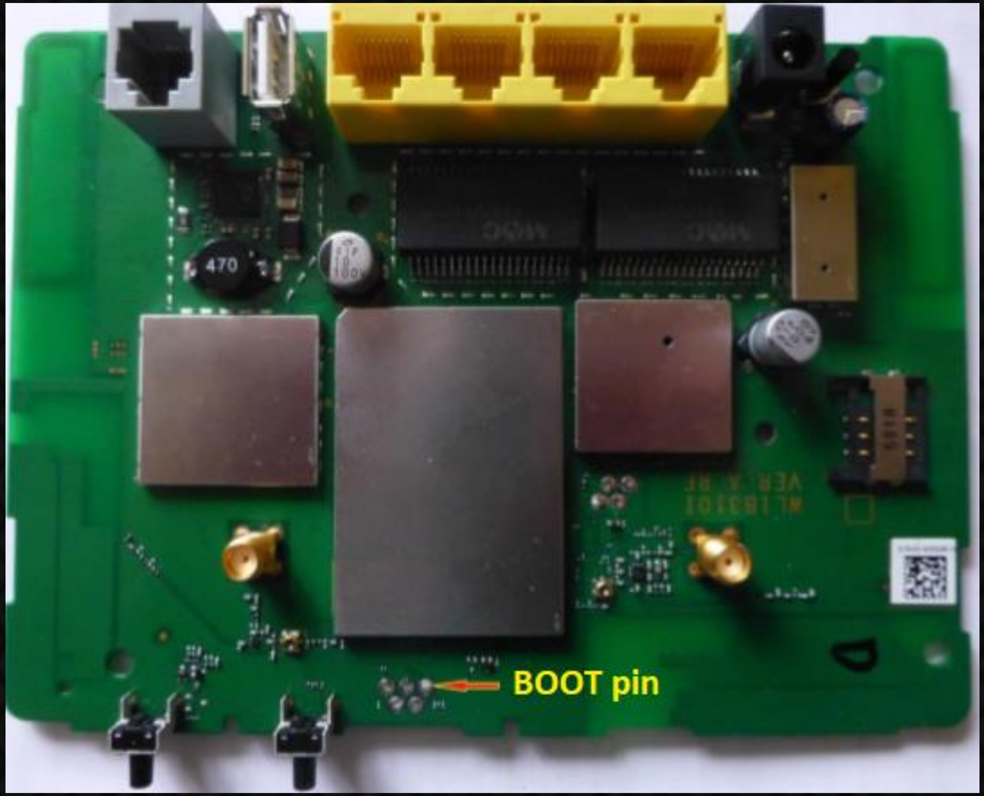
Exploitation Steps

1. Ensure WAN interface is active
2. Inject a new line into the PPTP VPN config to load a plugin
3. Compile a plugin to load
4. Upload plugin to spawn an ADB shell

./demo.sh

Huawei B315





root@router:/var/samba# cat smb.conf

```
[global]
   workgroup = WORKGROUP
   netbios name = huawei.com
   server string = samba server
   …
   dfree command = /var/hax.sh
[hax]
   path = /mnt/sdcard/%m/%m/var
   valid users = hax
   writeable = yes
   printable = no
```

2 - execute shell script

1 - directory path traversal

Exploitation Steps

1. Create a new SMB share
2. Inject the %m variable into the path
3. Connect to the share with a NETBIOS name of “..”
4. Edit smb.conf to run adbd

HACK THE PLANET[1]

[1]demo

:q