Gaining root privileges on a Netgear M1 Mobile Router (MR1100)

Michael Callahan · Follow

3 min read · Aug 30, 2021

This article will (hopefully) be part 1 of 2, covering the broader topic of converting an AT&T business/enterprise model hotspot into a normally

functioning Netgear generic hotspot. I am not liable if you break your things. Information purposes only.

Firmware version and background

Thanks to a DefCon talk (here) a vulnerability was disclosed allowing arbitrary command injection using the Netgears config api. Using this slide deck I was able to piece together the rest of the process.

Enabling telnet

The first step is to make sure telnet is enabled. If you have a generic Netgear mobile hotspot, you can skip this step. If you have an AT&T business model, your USB tethering doesn't work. To enable USB functionality, connect to your mobile hotspot using wifi and navigate to http://192.168.1.1. Then do the following:

1. Login with your username and password (default is username: *blank* password: **attadmin**
2. Navigate to settings -> administration -> backup settings
3. Click backup settings
4. Open the downloaded config file in a text editor and add *router.usbNetworkTethering=true* to the end of the file and save it
5. Use the same page to import this new config file

USB tethering should now be partially enabled. You will be able to telnet into the hotspot over USB but not access the internet.

Flashing the firmware

You will need a few pieces of software to flash firmware.

Download the vulnerable generic firmware: https://www.downloads.netgear.com/files/GDC/MR1100/MR1100-100NAS_23113828_NTG9x50C_12.05.05.00_00_GenericNA_01.02.secc.spk

Download FDT.exe version 4.6.2.0: https://www.dropbox.com/s/s27ftyfjpvn9819/fdt.exe?dl=0

Download AC78x Netgear drivers version 4.3.00: http://www.downloads.netgear.com/files/aircard/AC_790S_Telstra/AC78xSDrivers.exe

Download Putty: https://www.putty.org

1. Create a new folder and place all the files into it
2. Install the AC78x drivers
3. Remove the battery from your Netgear router (important)
4. Enter firmware flash mode by simultaneously holding the power button for 10 seconds and connecting the router to your pc using a USB-C cable. Don't release the power button until you see **Downloading software update**
5. Open a powershell window at the directory you placed the files (Shift-Right Click should give you an *open powershell window here* option)
6. Type *fdt.exe MR1100–100NAS_23113828_NTG9x50C_12.05.05.00_00_GenericNA_01.02.secc.spk*

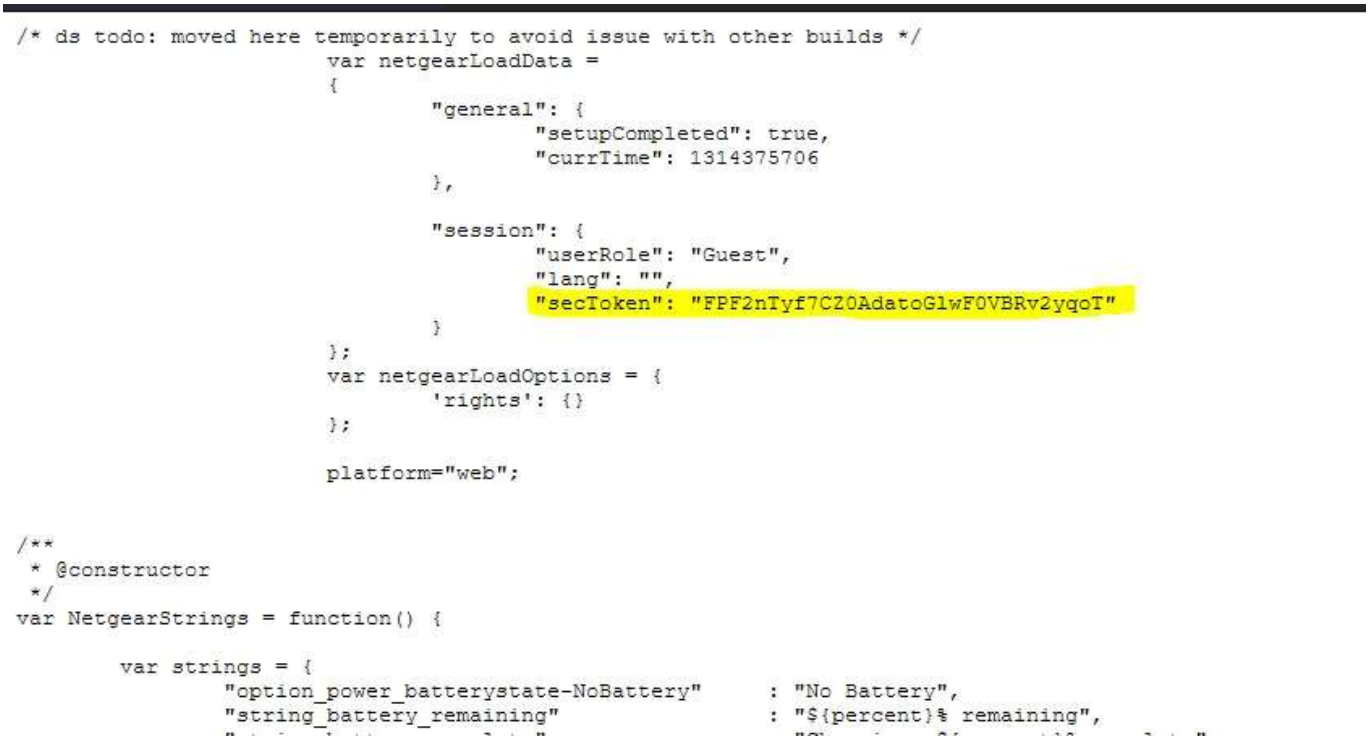
7. Wait for the update to finish

Gaining root

We are almost there. Now we just need to run the command injection. Navigate to http://192.168.1.1. The following process should be done in quick succession because the authentication token only lasts so long.

1. Authenticate first at the login page
2. Navigate to http://192.168.1.1/js/NetgearStrings.js

You should see a secToken value in the dictionary at the top of the page.



```
/* ds todo: moved here temporarily to avoid issue with other builds */
                        var netgearLoadData =
                        {
                                "general": {
                                        "setupCompleted": true,
                                        "currTime": 1314375706
                                },

                                "session": {
                                        "userRole": "Guest",
                                        "lang": "",
                                        "secToken": "FPF2nTyf7C20AdatoGlwF0VBRv2yqoT"
                                }
                        };
                        var netgearLoadOptions = {
                                'rights': {}
                        };

                        platform="web";


/**
 * @constructor
 */
var NetgearStrings = function() {

        var strings = {
                "option_power_batterystate-NoBattery"     : "No Battery",
                "string_battery_remaining"                : "${percent}% remaining",
```

3. Copy this secToken into notepad

4. Copy this command into notepad http://192.168.1.1/Forms/config?ready.deviceShare.removeUsbDevice=%3B%24(busybox%20telnetd)%3B&err

_redirect=/error.json&ok_redirect=/success.json&token=

5. Place your secToken at the end of the equals sign ex. (http://192.168.1.1/Forms/config?ready.deviceShare.removeUsbDevice=%3B%24(busybox%20telnetd)%3B&err_redirect=/error.json&ok_redirect=/success.json&token=FPF2nTyf7CZ0AdatoGlwF0VBRv2yqoT)

6. Paste the final command in your browser. If it worked you should see {success: true} displayed

7. Open Putty and telnet into 192.168.1.1 port **23. (Not port 5510)**

8. You should be prompted with a shell login

Username is **root**

Password is **oelinux123**

All done!

Congrats! You now have root access to the filesystem. You can use most shell commands. Have fun looking around.

Netgear Mobile Hotspot

Written by Michael Callahan

Follow

10 Followers

Strategic Cloud Engineer at Google. Passionate about security and cloud infrastructure. All views are my own.

More from Michael Callahan

Michael Callahan

Generating an elliptic curve certificate authority

There are a lot of articles about generating SSL/TLS certificates. There are few articles ...

2 min read · Mar 24, 2023

Michael Callahan

Azure Web App With Postgres: Fixing Slow PHP Load Times

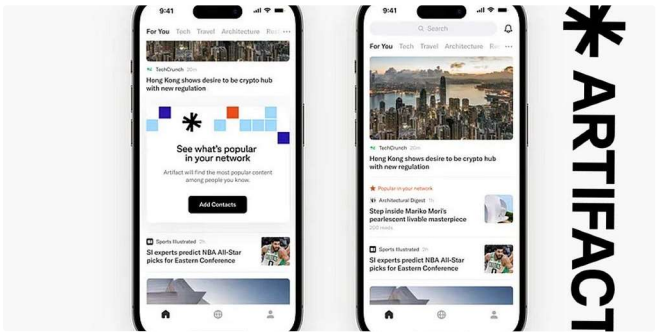
Background Feel free to jump to the bottom if you just want to see the solution. Big thanks...

3 min read · May 15, 2020

14 1

See all from Michael Callahan

Recommended from Medium



James Presbitero Jr. in Practice in Public

These Words Make it Obvious That Your Text is Written By AI

These 7 words are painfully obvious. They make me cringe. They will make your reader...

4 min read · Dec 31, 2023

33K 866

Gowtham Oleti

Apps I Use And Why You Should Too.

Let's skip past the usual suspects like YouTube, WhatsApp and Instagram. I want t...

10 min read · Nov 14, 2023

16.4K 284

Lists

Staff Picks

570 stories · 706 saves

Stories to Help You Level-Up at Work

19 stories · 453 saves

Self-Improvement 101

20 stories · 1292 saves

Productivity 101

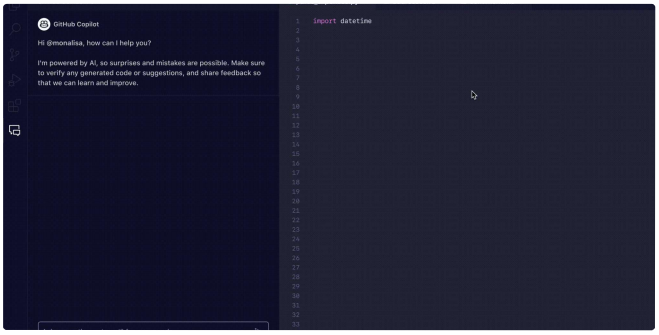
20 stories · 1184 saves

Unbecoming

10 Seconds That Ended My 20 Year Marriage

It's August in Northern Virginia, hot and humid. I still haven't showered from my...

· 4 min read · Feb 16, 2022



Jacob Bennett in Level Up Coding

The 5 paid subscriptions I actually use in 2024 as a software engineer

Tools I use that are cheaper than Netflix

· 5 min read · Jan 4

74K 1051 6.4K 76

ScriptMint

My MacBook Setup for Development (2024)

For the past two years, I've been sharing my MacBook setup for development, and I'm...

8 min read · Jan 15

1.5K 31

Scott-Ryan Abt in Pitfall

Bye Bye, Spotify

And see ya later, all you subscription services in my little empire

· 4 min read · Aug 19, 2023

19.3K 446

See more recommendations