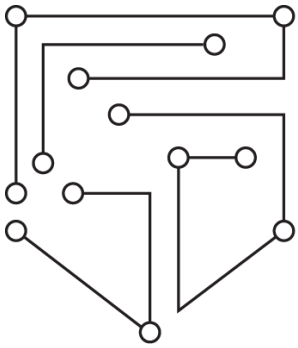


ST. CYR
SECURITY

St. Cyr Security Product Security Advisory

Hardware	Torch WiFi Router
Vendor	Torch (https://mytorch.com/)
Version Tested	1.5.7 (1.6.3 current, also vuln)
Vulnerability Type	Multiple vulnerabilities
Severity	Critical
Date	May 9, 2017

Background:

St. Cyr Security, LLC has discovered the following vulnerabilities in the Torch Router implementation while reviewing the device security prior to deployment. This is not meant to be a comprehensive assessment of the hardware device. The vendor was notified on Feb 26, 2017 that there were vulnerabilities to discuss, however vendor was not ready to accept the findings report. Vendor never re-established communication to determine vulnerabilities. On May 9, 2017, customers were notified that the company was ceasing operations and on May 31, 2017 the routers will no longer function.

Risk Assessment:

These routers are built to be centrally managed by the mytorch.com website and contain no user controlled interface on the device itself. The API (api.mytorch.com) is accessed with an insecure (http) protocol, no authentication, and authorization based on the LAN MAC address of the device. If a device error occurs, the device log files are sent to a Gmail account utilizing a hard-coded password, from the same email account.
The purpose of this device is to help parents control their children's Internet connection, however the device leaks data on those children.

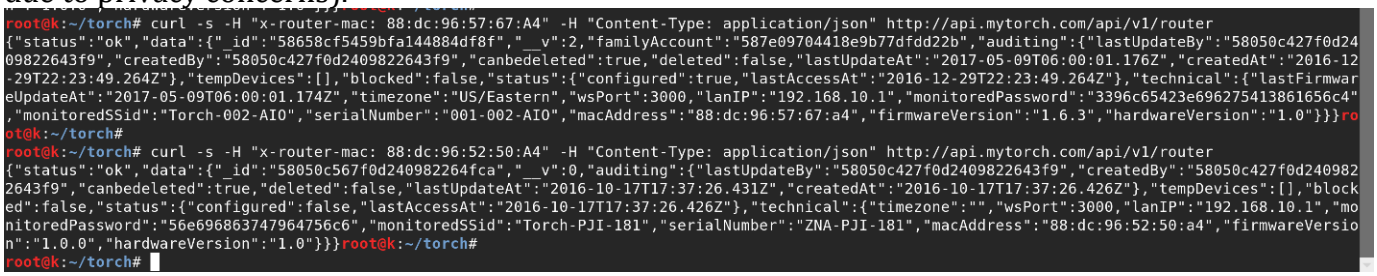
Vulnerabilities:

The following is a technical description of each individual vulnerability.

No Authentication, Guessable Authorization:

When the Torch Wifi Router communications with http://home.mytorch.com/api/ and http://api.mytorch.com/api, it does so utilizing an 'x-router-mac' header. There is no authentication required, and the header handles the authorization to view the router's config file. Simply knowing (or guessing) the MAC address can allow an attacker to gain knowledge of the firmware installed on the device, the Wifi SSID, Wifi password, time zone, serial number, and profiles. These profiles are typically children's names, and contains a list of their device names and mac addresses.

The following screenshots show the API calls for 2 randomly guessed MAC addresses within known ranges to get device information (profiles data not shown due to privacy concerns).



Hardcoded Gmail Credentials:

During the firmware update process, if an error is encounter, the log files from the devices are emailed to torchrouter@gmail.com from torchrouter@gmail.com utilizing a hardcoded password which can be found in /etc/config/msmtp.
This password was NOT verified as being valid, however the company was made aware of this vulnerability on Feb 26, 2017.

```
root@k:~/torch/1.6.3/_ab759971be6036447f29a38d0d97de03.bin.extracted/squashfs-root/etc/config# cat msmtp
account default

host smtp.gmail.com
port 587
auth on
user torchrouter@gmail.com
password torchrouter!

auto_from off
from torchrouter@gmail.com

tls on
tls_starttls on
tls_certcheck off

logfile
syslog LOG_MAIL
```

Improperly Protected Sensitive Data:

The API call to http://api.mytorch.com/api/v1/router retrieves the variable 'monitoredPassword'. This is then piped to *rev* (reverse), and *xxd* (un-hex), to obtain the cleartext of the password for the WiFi access.
The following screenshot shows the code in action on /etc/torch/update_config

```
    if [ -n "$monitoredSsid" ] && [ -n "$monitoredPassword" ]; then
        # decrypt wifi hash
        #RESULT=$($TORCHCRYPT "$passwd")
        #UNMONIT_PASS=$(echo "$unmonitoredPassword" | rev | xxd -r -p)
        MONIT_PASS=$(echo "$monitoredPassword" | rev | xxd -r -p)
        # and check if result is OK
        if [ $? -eq 0 ]; then
            echo [`$TIMESTAMP`"] SUCCESS decrypt hash wifi ... !" >> $LOGFILE
            echo [`$TIMESTAMP`"] $MONIT_PASS / $UNMONIT_PASS " >> $LOGFILE
            # invers netwrok for lan unmonitored
            # same wifi for both interface
```

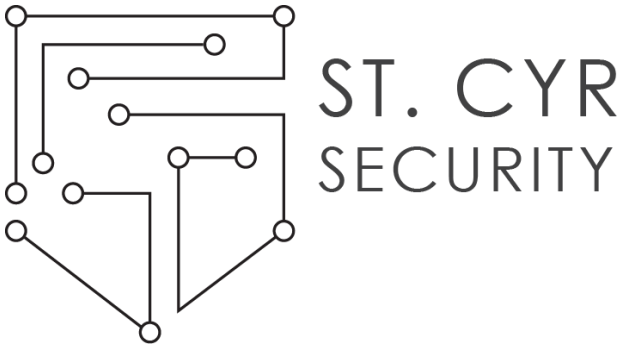
Insecure Communication Channel:

The /etc/config/torchdomains config file contains a list of domains the router connects to. None of the domains communicate a secure http**s** connection, instead all utilizing HTTP. This was manually verified in action on the network when connecting the device to a MONITOR/SPAN port.
Of most concern are the two URLs which contain config and sensitive user information:

- http://home.mytorch.com
- http://api.mytorch.com

This allows for the connection to be eavesdropped and altered by ISPs, Nation-state level actors, or an attacker utilizing a man-in-the-middle attack.

```
root@k:~/torch/1.5.7/_d89045f5e78dd501fd3cf3c1bfdc8490.bin.extracted/squashfs-root/etc/config# cat torchdomains
torchdomain=http://home.mytorch.com
torchapi=http://api.mytorch.com
my_torch=http://home.mytorch.com
torchos=http://192.168.10.1
firstsetup=/router/setup
devicesetup=/device
api_devices_all=/api/v1/devices
api_devices_add=/api/v1/devices
api_devices_blacklist=/api/v1/devices/blacklist
api_traffic=/api/v1/devices/traffic
api_config_all=/api/v1/router
api_blacklist_all=/api/v1/blacklist
api_profiles=/api/v1/profiles
api_blocking=/api/v1/devices/blocking
api_firmware=/api/v1/router/firmware
dns='52.45.212.122 52.45.225.194'
log_email="weknodeit@gmail.com"
root@k:~/torch/1.5.7/_d89045f5e78dd501fd3cf3c1bfdc8490.bin.extracted/squashfs-root/etc/config#
```



Disclosure Timeline:

St. Cyr Security follows the US-CERT's policy on disclosing to the public the existence of vulnerabilities **45** days after being reported to the US-CERT or vendor. Similar to the US-CERT, St. Cyr Security may adjust the publication schedule based on the circumstances of the vulnerabilities being disclosed. Due to the company closing, and the possibility for devices to be taken over by these vulnerabilities in less than **45** days, the disclosure to US-CERT is being made.

Credit:

Mike Cyr (h00die)

- mike@stcyrsecurity.com