Another LILIN DVR 0-day being used to spread Mirai

blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/

Genshen Ye

December 3, 2020

3 December 2020 / 0-day

Author: Yanlong Ma, Genshen Ye

Background Information

In March, we reported[1] that multiple botnets, including Chalubo, Fbot, Moobot were using a same 0 day vulnerability to attack LILIN DVR devices, the vendor soon fixed the vulnerability.

On August 26, 2020, our Anglerfish honeypot detected that another new LILIN DVR/NVR 0-day paired with system default credential operxxxx:xxxxx(masked for security concern) were used to spread Mirai sample.

On September 21, 2020, we reported the finding to the Merit LILIN contact, and the vendor fixed the vulnerability overnight, and also provided us a firmware fix ver 4.0.26.5618.

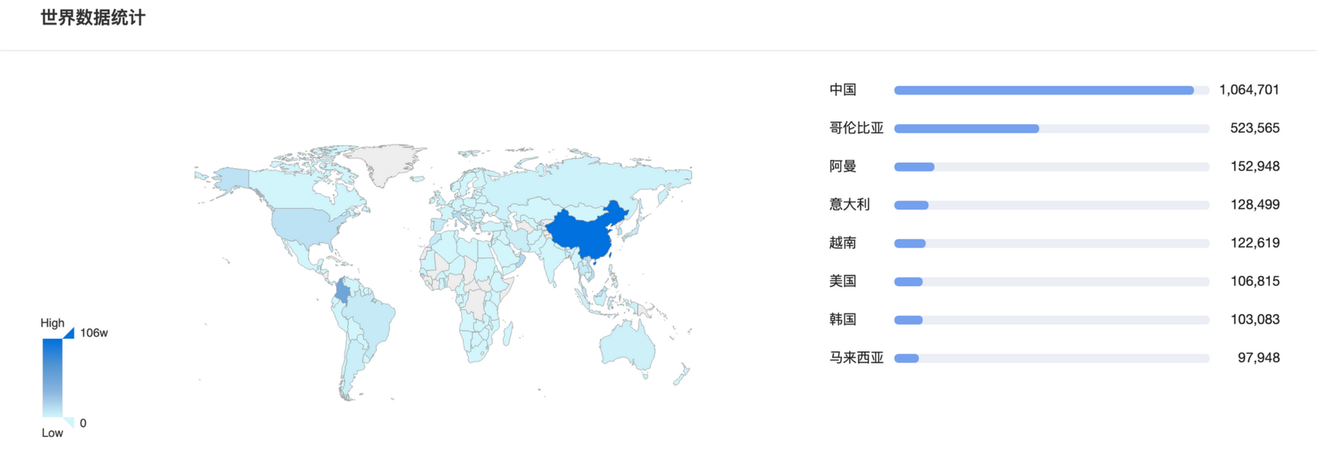
Impact devices

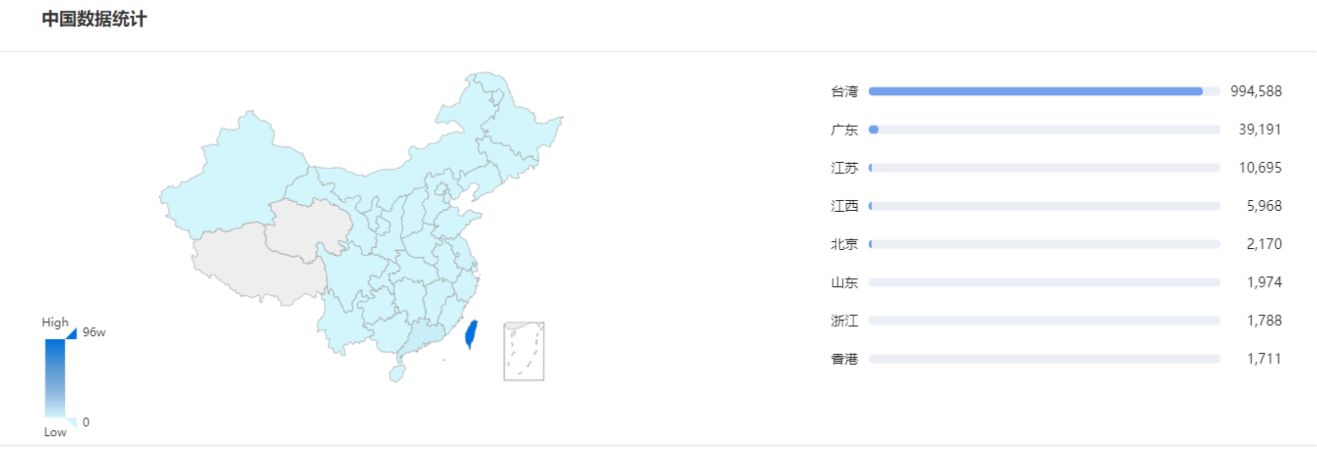
The 360 FirmwareTotal system provides the following firmware list that are impacted.

```
DH032 Firmware v1.0.26.3858.zip
DH032 Firmware v1.0.28.3858.zip
DVR708 Firmware v1.3.4.zip
DVR716 Firmware v1.3.4.zip
DVR816 Firmware v1.3.4.zip
Firmware-DH032-EN.zip
Firmware-DVR708-EN.zip
Firmware-DVR716-EN.zip
Firmware-DVR816-EN.zip
Firmware-NVR100L-EN.zip
Firmware-NVR1400-EN.zip
Firmware-NVR200L-EN.zip
Firmware-NVR2400-EN.zip
Firmware-NVR3216-EN.zip
Firmware-NVR3416-EN.zip
Firmware-NVR3416R-EN.zip
Firmware-NVR3816-EN.zip
Firmware-NVR400L-EN.zip
Firmware-NVR5104E-EN.zip
Firmware-NVR5208E-EN.zip
Firmware-NVR5416E-EN.zip
Firmware-NVR5832-EN.zip
Firmware-NVR5832S-EN.zip
NVR 404C Firmware v1.0.48.zip
NVR 404C Firmware v1.0.56.zip
NVR 408M Firmware v1.0.56.zip
NVR100L 200L Rescue File.zip
NVR100L Firmware v1.1.56 - HTML5 Version.zip
NVR100L Firmware v1.1.66.zip
NVR100L Firmware v1.1.74 - Push Notification Fix.zip
NVR100L, 200L Rescue File.zip
NVR100LFirmware.zip
NVR104 Firmware v1.0.48.zip
NVR104 Firmware v1.0.56.zip
NVR109 Firmware v1.0.38.zip
NVR109 Firmware v1.0.48.zip
NVR109 Firmware v1.0.56.zip
NVR116 Firmware v1.0.38.zip
NVR116 Firmware v1.0.48.zip
NVR116 Firmware v1.0.56.zip
NVR1400Firmware.zip
NVR1400L Firmware v1.1.56 - HTML5 Version.zip
NVR1400L Firmware v1.1.66.zip
NVR1400L Firmware v1.1.74 - Push Notification Fix.zip
NVR200L Firmware v1.1.56 - HTML5 Version.zip
NVR200L Firmware v1.1.66.zip
NVR200L Firmware v1.1.74 - Push Notification Fix.zip
NVR200LFirmware.zip
NVR2400Firmware.zip
NVR2400L Firmware v1.1.56 - HTML5 Version.zip
NVR2400L Firmware v1.1.66.zip
NVR2400L Firmware v1.1.74 - Push Notification Fix.zip
NVR3216 Firmware v3.0.74.3921.zip
NVR3216 Recovery Tool.zip
NVR3416 Firmware v3.0.74.3921.zip
```

```
NVR3416 Recovery Tool.zip
NVR3416r Firmware v3.0.76.3921.zip
NVR3816 Firmware v2.0.74.3921.zip
NVR400L 1400 2400 Rescue File.zip
NVR400L Firmware v1.1.56 - HTML5 Version.zip
NVR400L Firmware v1.1.66.zip
NVR400L Firmware v1.1.74 - Push Notification Fix.zip
NVR400L, 1400, 2400 Rescue File.zip
NVR5104E Firmware v5.0.24.4078.zip
NVR5104E Recovery Tool.zip
NVR5208E Firmware v5.0.24.4078.zip
NVR5208E Recovery Tool.zip
NVR5416E Firmware v4.0.24.4078.zip
NVR5832 Firmware v4.0.24.4043.zip
NVR5832 Firmware v4.0.24.4043.zip
NVR5832 Recovery Tool.zip
NVR5832S Firmware v4.0.24.4043.zip
NVR5832S Recovery Tool.zip
VD022 Firmware 1.0.48.zip
VD022 Firmware 1.0.56.zip
```

The 360 Quake cyberspace mapping system mapped assets across the global and discovered that there are 1049094 IP addresses of devices with Merit LILIN DVR/NVR fingerprints (app:"LILIN_DVR") on the public network, and 6748 of them are considered vulnerable. The vast majority of these devices are located in Taiwan, China, as shown in the figure below.





Vulnerability Analysis

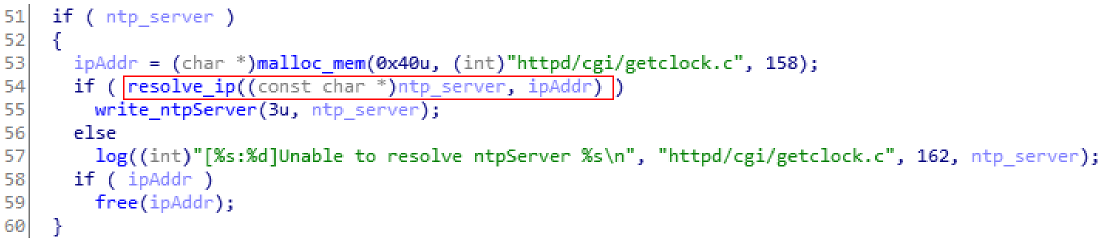
Vulnerability Type: Remote Command Execution Vulnerability
Vulnerability detail: The Web service program `/opt/extra/main` defines a `GET /getclock` interface for viewing and modifying time-dependent device configurations. When the `/opt/extra/main` program is started, the command line program `/mnt/mtd/subapp/syscmd` is started and the commands that need to be executed are passed to syscmd via shared memory.

1. When the value of the incoming parameter cmd is set, the parameter NTP_SERVER can be used to set the time synchronization server for the device.
2. The `GET /getclock` callback function does not check the value of NTP_SERVER and saves the relevant fields, then it creates a `CMDQ_SET_SYS_TIME` message to be pressed into cmdQueue.
3. The corresponding `CMDQ_SET_SYS_TIME` message processing function of cmdQueue reads the relevant fields and splices the following shell command into the shared memory, resulting in a remote command execution vulnerability.

```
/opt/extra/subapp/ntpclient -s -t -h %s > %s &", v4, "/tmp/ntp.dat"
```

Vulnerability Fix: In the updated firmware, we notice that before saving the `NTP_SERVER` parameter, the `resolve_ip()` function is called to encapsulate the `inet_aton()` function to check if the input is a correct IP address.
The process is as follows.

1. For parameters in URL format, `libadns.so` library is called for domain name resolving, if it success, the ip address is written into ipAddr and return True; otherwise return False.
2. For IP addresses, write directly to ipAddr and return True.



```
if ( ntp_server )
{
  ipAddr = (char *)malloc_mem(0x40u, (int)"httpd/cgi/getclock.c", 158);
  if ( resolve_ip((const char *)ntp_server, ipAddr) )
    write_ntpServer(3u, ntp_server);
  else
    log((int)"[%s:%d]Unable to resolve ntpServer %s\n", "httpd/cgi/getclock.c", 162, ntp_server);
  if ( ipAddr )
    free(ipAddr);
}
```

Recommendations

We recommend that Merit LILIN DVR/NVR users check and update the firmware system and set strong login credentials for the devices.

We recommend users monitor and block the urls on the IoC list.

Contact us

Readers are always welcomed to reach us on **twitter**, or email to netlab at 360 dot cn.

IoC list

MD5

```
0bf1fd0cfa9ced2d95e17f4d9cf10d34
1c3b2a0738476c609656515c5422002e
1c7735dba999c106197bb8defb143925
1f56696725930ae35428fbdb7c953ce0
2b1e0f7a3fcf3478ea726a3b04a9e601
6e90346591e95a623c8a16695c1b36cd
7d8fb579f1d3a4320fcc5e712970d84e
8b8800449bf9729e00b41729632699f6
8f481d0da94b964e4061cd96892386d4
20b89f0640215b0180b357ce2d07dc10
43c477a3df65c2ecd4580dc944208d59
51de7b96b43a4062d578561becff713c
60d6a7a725221e7772dbd192aaa3f872
267e120fc765784f852ed6b2fa939f46
614ca6d9c18fe15db1e8683c9e5caeb8
64714ff03f088a9702faf9adbdc9f2d6
32887409ed42e8e6df21c5600e572102
a18266a67bbf45d8bb19bd6f46519587
afdb1f3312b3029143e9f2d09b92f2a1
ce8bf6ed38037792e25160a37b23cd4f
f9887d332e35f9901ef507f88b5e06cb
fcaff61a5de5e44083555a29ee4f5246
feaf1296790d3e1becef913add8ba542
```

URL

```
http://2.57.122.167:5858/f
http://2.57.122.167:5858/uwu/arm
http://2.57.122.167:5858/uwu/arm5
http://2.57.122.167:5858/uwu/arm6
http://2.57.122.167:5858/uwu/arm7
http://2.57.122.167:5858/uwu/m68k
http://2.57.122.167:5858/uwu/mips
http://2.57.122.167:5858/uwu/mpsl
http://2.57.122.167:5858/uwu/ppc
http://2.57.122.167:5858/uwu/sh4
http://2.57.122.167:5858/uwu/spc
http://2.57.122.167:5858/uwu/x86
http://2.57.122.167:5858/webos/whoareyou.arm
http://2.57.122.167:5858/webos/whoareyou.arm5
http://2.57.122.167:5858/webos/whoareyou.arm6
http://2.57.122.167:5858/webos/whoareyou.arm7
http://2.57.122.167:5858/webos/whoareyou.m68k
http://2.57.122.167:5858/webos/whoareyou.mips
http://2.57.122.167:5858/webos/whoareyou.mpsl
http://2.57.122.167:5858/webos/whoareyou.ppc
http://2.57.122.167:5858/webos/whoareyou.sh4
http://2.57.122.167:5858/webos/whoareyou.spc
http://2.57.122.167:5858/webos/whoareyou.x86
```

IP

2.57.122.167	Romania	ASN48090	Pptechnology Limited