0-day

LILIN DVR/NVR 在野0-day漏洞攻击报告2

Genshen Ye
Dec 3, 2020 • 6 min read

本文作者：马延龙，叶根深

背景介绍

2020年8月26号，360网络安全研究院Anglerfish蜜罐系统监测到有攻击者，使用Merit LILIN DVR/NVR 默认密码和0-day漏洞，传播Mirai僵尸网络样本。

2020年9月25号，Merit LILIN联络人在收到漏洞报告后，快速地响应并提供了固件修复程序(4.0.26.5618 firmware version for NVR5832)。

此前，我们曾向Merit LILIN报告了另一个0-day漏洞[1][2]。

时间线

```
2020年9月21号，我们邮件联系Merit LILIN厂商并报告了漏洞详情以及在野攻击PoC。
2020年9月22号，Merit LILIN联络人邮件回复已经连夜修复该问题。
2020年9月25号，Merit LILIN联络人提供固件修复程序4.0.26.5618 firmware version for NVR5832。
```

影响范围

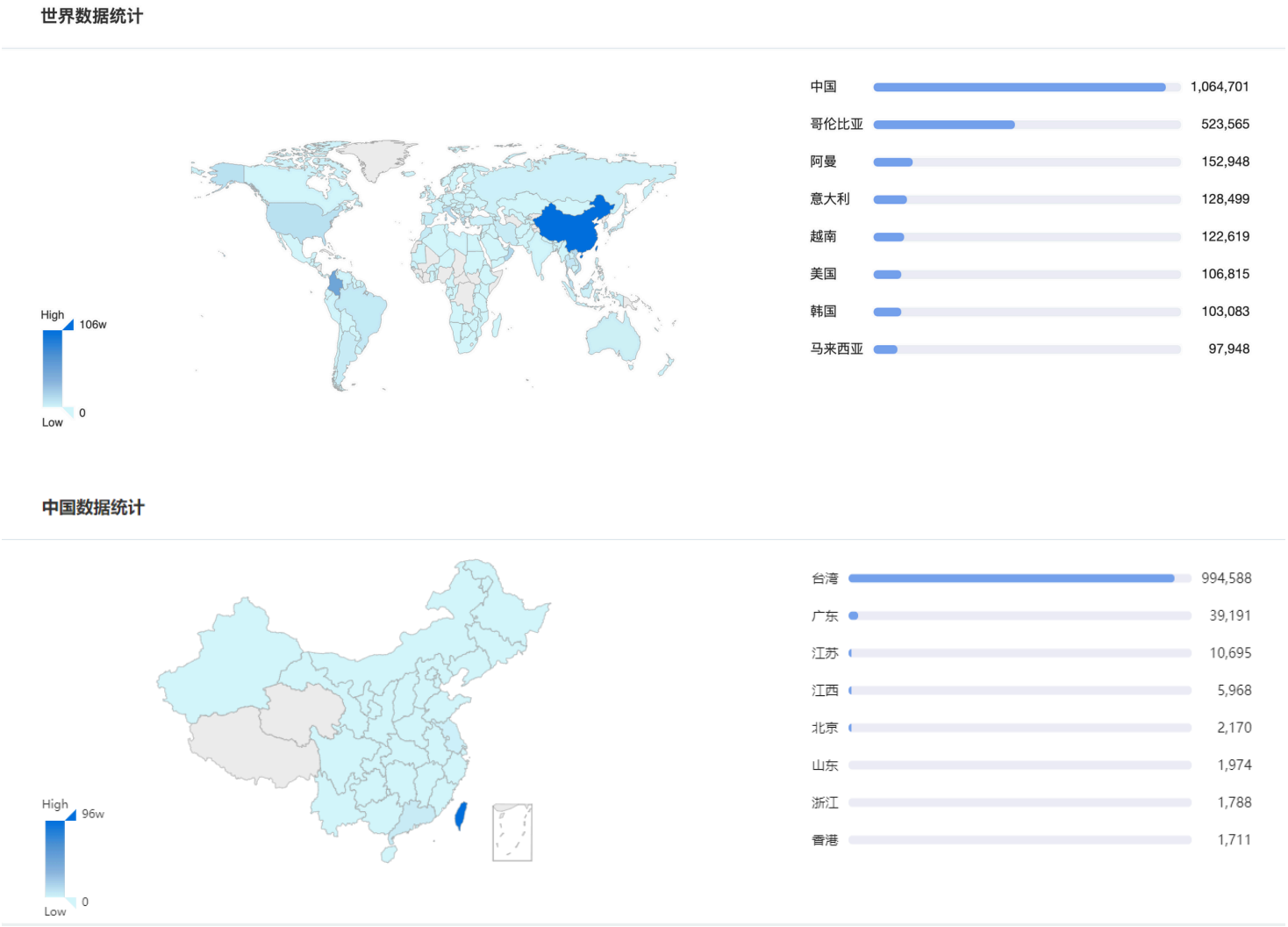
360 FirmwareTotal系统通过对Merit LILIN DVR/NVR固件分析和漏洞验证，发现以下固件受影响。

```
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
```

360 Quake网络空间测绘系统通过对全网资产测绘，发现公网上存在Merit LILIN DVR/NVR指纹(app:"LILIN_DVR")的设备共有1049094个IP地址，符合上述固件指纹特征的IP共有6748个。其中大部分设备位于在中国台湾省，具体分布如下图所示。



漏洞分析

漏洞类型: 需授权的远程命令执行漏洞
漏洞原因: Web服务程序 `/opt/extra/main` 定义了 `GET /getclock` 接口，用于查看和修改设备时间相关配置。当 `/opt/extra/main` 程序启动时，会启动命令行程序 `/mnt/mtd/subapp/syscmd` ，将需要执行的命令通过共享内存交由 `syscmd` 执行。

1. 当传入参数 `cmd` 的值为 `set` 时，可以使用参数 `NTP_SERVER` 设置设备的时间同步服务器。
2. 由于 `GET /getclock` 接口的回调函数，并未对参数 `NTP_SERVER` 的值进行过滤，即将相关字段保存，并创建 `CMDQ_SET_SYS_TIME` 消息压入cmdQueue。
3. cmdQueue对应的 `CMDQ_SET_SYS_TIME` 消息处理函数读取相关字段，并拼接如下shell命令，写入共享内存，导致远程命令执行漏洞。

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

漏洞修复：在固件修复程序中，我们看到保存 `NTP_SERVER` 参数前，会调用 `resolve_ip()` 函数封装 `inet_aton()` 函数判断该参数值是否为正确的IP地址。具体修复过程如下:

1. 对于URL格式的参数，调用libadns.so库进行域名解析，若解析成功，则将地址写入ipAddr，返回True；否则返回False
2. 对于IP地址，则直接写入ipAddr，返回True

处置建议

我们建议Merit LILIN DVR/NVR用户及时检查并更新固件系统，同时给设备设置复杂的登录密码。

我们建议读者对相关IP和URL进行监控和封锁。

联系我们

感兴趣的读者，可以在 twitter 或者通过邮件netlab[at]360.cn联系我们。

IoC list

样本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
```

— 360 Netlab Blog - Network Security Research Lab at 360 —

0-day

EwDoor僵尸网络，正在攻击美国AT&T用户

EwDoor Botnet Is Attacking AT&T Customers

一个藏在我们身边的巨型僵尸网络 Pink

See all 22 posts →

0-day

Another LILIN DVR 0-day being used to spread Mirai

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/

Dec 3, 2020 · 5 min read

Import 2022-11-30 11:16

DNS data mining case study - skidmap

As the foundation and core protocol of the Internet, the DNS protocol carries data that, to a certain extent, reflects a good deal of the user behaviors, thus security analysis of DNS data can cover a decent amount of the malicious activities.

In the early days, typical scenarios for early

Nov 30, 2020 · 9 min read