LILIN DVR

Multiple botnets are spreading using LILIN DVR 0-day

Alex.Turing, Genshen Ye
Mar 20, 2020 • 4 min read

Author: Yanlong Ma, Lingming Tu, Genshen Ye, Hongda Liu

When we talk about DDos botnet, we tend to think the typical scenario, some mediocre, code-borrowing scripts target old vulnerabilities. But things actually have started to change, we noticed more and more attackers beginning to use 0-day vulnerabilities.

Background

Starting from August 30, 2019, 360Netlab Threat Detection System has flagged multiple attack groups using LILIN DVR 0-day vulnerabilities to spread Chalubo[1], FBot[2], Moobot[3] botnets.

On January 19, 2020, we reached out to the equipment manufacturer LILIN. On February 13, 2020, the vendor fixed the vulnerability[4], and released the latest firmware program 2.0b60_20200207[5].

Vulnerability analysis

The LILIN 0-day vulnerability is made of 3 parts: hard-coded login credentials, `/z/zbin/dvr_box` command injection vulnerabilities and `/z/zbin/net_html.cgi` arbitrary file reading vulnerabilities, `/z/zbin/dvr_box` provides Web services, and its web interface `/dvr/cmd` and

`/cn/cmd` have a command injection vulnerability. The injected parameters have been: NTPUpdate, FTP, and NTP.

List of hardcoded login credentials:

```
root/icatch99
report/8Jg0SR8K50
```

Default login credentials:

```
admin/123456
```

NTPUpdate injection vulnerability analysis

1. `/z/zbin/dvr_box` The `dvr_serv::do_request()` function is responsible for parsing the `DVRPOST` incoming XML configuration and calling the corresponding processing function;
2. `dvr_core::NTPUpdate()` The processing function passes the Server field into a function in the dependent library libutility.so `UtilityBox::UtilityNtp::run()`;
3. `UtilityBox::UtilityNtp::run()` The function splices and executes the ntp time synchronization command according to the value of the Server field;
4. The above process chain does not filter special characters in the Server field, command injection becomes possible.
   In the newly patched version `2.0b60_20200207`, the vendor fixed the vulnerability by calling `UtilityBox::Utility::ValidateHostName()` to
   checks the Server field at step 3

```
signed int __fastcall UtilityBox::UtilityNtp::run(UtilityBox::UtilityNtp *this, const char *Server)
{
  UtilityBox::Utility *v2; // r6
  int v3; // r5
  const char *server; // r1
  const char *v6; // r1
  int v7; // r5
  int v8; // r0
  int v9; // [sp+0h] [bp-30h]
  char v10; // [sp+10h] [bp-20h]
  UtilityBox::Utility *v11; // [sp+1Ch] [bp-14h]

  v2 = (UtilityBox::Utility *)Server;
  if ( !*((_DWORD *)this + 34) )
    return -1;
  if ( !Server )
    return -1;
  if ( !j_strlen1((int *)Server) )
    return -1;
  if ( !UtilityBox::Utility::ValidateHostName(v2, server) )
    return -1;
  UtilityBox::UtilityString::UtilityString((UtilityBox::UtilityString *)&v10, "msntp -V -c 1 -r %s", v2);
  v7 = UtilityBox::Utility::system(v11, v6);
```

FTP and NTP injection vulnerability analysis

1. Device configuration `/zconf/service.xml`, can be obtained through hard-coded login account password and `/z/zbin/net_html.cgi` arbitrary file reading [6];
2. By modifying the Server field of the FTP or NTP parameters in the `/zconf/service.xml`, backdoor command can be injected;
3. Remotely access the `/dvr/cmd` interface through hard-coded account passwords, then use the SetConfiguration function to upload the modified XML entity, now the configuration files can be written to the target device
4. The device periodically synchronizes the FTP or NTP configuration, which triggers the command execution.

It is worth noting that the command injection for FTP or NTP configuration relies on the network configuration obtained in steps 1 and 2. If step 3 is executed directly, the device will come offline.

In the newly patched version `2.0b60_20200207`, the vendor has fixed this vulnerability, `/z/zbin/dvr_box` now calls the `UtilityBox::Utility::ValidateHostName()` function to check the Server field when writing the configuration.

```
462         v79 = (const char *)tinyxml2::StrPair::GetStr((tinyxml2::StrPair *)(v6 + 12));
463         if ( !strcmp(v79, "NTP") )
464         {
465           v122 = (int *)tinyxml2::XMLElement::Attribute((tinyxml2::XMLElement *)v6, "Enable", 0);
466           v124 = UtilityBox::Utility::set((dvr_xml_service *)((char *)v3 + 1084), v122, v123) | v7;
467           v125 = (int *)tinyxml2::XMLElement::Attribute((tinyxml2::XMLElement *)v6, "Interval", 0);
468           v7 = v124 | UtilityBox::Utility::set((dvr_xml_service *)((char *)v3 + 1088), v125, v126);
469           v127 = (UtilityBox::Utility *)tinyxml2::XMLElement::Attribute((tinyxml2::XMLElement *)v6, "Server", 0);
470           if ( UtilityBox::Utility::ValidateHostName(v127, v128) )
471           {
472             v129 = (char *)tinyxml2::XMLElement::Attribute((tinyxml2::XMLElement *)v6, "Server", 0);
473             v11 = UtilityBox::Utility::set((dvr_xml_service *)((char *)v3 + 1092), v129, v130);
474             goto LABEL_7;
475           }
476         }
```

Timeline

```
2019/08/30 We discovered Chalubo was spreading through the LILIN 0-day NTPUpdate vul
2020/01/11 We discovered that FBot was spread through the LILIN 0-day FTP / NTP vulne
2020/01/19 We reached out to the vendor.
2020/01/26 We discovered that Moobot was spreading through the LILIN 0-day FTP vulne
2020/02/10 We reached out to the vendor again.
2020/02/12 We provided the FTP and NTP 0 day PoC details to the vendor.
2020/02/14 Vendor replied and fixed the vulnerability, and a new firmware 2.0b60_202
```

Affected firmware list

```
LILIN DHD516A
* 2.0b1_20191202 - JPEG C4 panels
* 2.0b1_20180828  - RTSP works

LILIN DHD508A
* 2.0b1_20180828  - RTSP works

LILIN DHD504A
* 2.0b1_20191202 - JPEG C4 panels
* 2.0b1_20190417  - JPEG C4 panels

LILIN DHD316A
* 2.0b1_20180828
* 2.0b1_20171128 C4 Panels

LILIN DHD308A
* 2.0b1_20180828

LILIN DHD304A
* 2.0b1_20180828

LILIN DHD204 IP  Camera
* 1.06_20151201

LILIN DHD204A IP Camera
```

```
* 2.0b60_20160223
* 2.0b60_20161123

LILIN DHD208 IP Camera
* 2.0b60_20160504

LILIN DHD208A IP Camera
* 2.0b60_20160223
* 2.0b60_20161123

LILIN DHD216 IP Camera
* 2.0b60 20151111

LILIN DHD216A IP Camera
* 2.0b60_20160223
* 2.0b60_20161123
```

Suggestions

LILIN users should check and update their device firmwares in a timely fashion, and strong login credentials for the device should be enforced.

The relevant malicious IPs, URLs and domains should be blocked and investigated on users'network.

Contact us

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

IoC list

MD5

```
0bf499baf3f0e623975a54225e9bd1a9
0d5193bdf74c87a14696f320d6808077
0f863f624da0d74094cb0f91cc226281
10ac26ef8571896efa3ee9495c0b71f5
164cc07fe71cd4db13133743e13612d8
20e8dd1fa2cc5e05ed2052c543f91ce1
21023609945be3f70459d30d1eec662e
267115637ef139b67007ee357c5397f6
3085b8f16c1ee686aa3bc3d1a91803f4
```

```
47e005e3136430452a0626b82f59ce15
4b87280c0b1b2b975c4f7412499400f2
502020b53b7bc053e0e3d8b85b5e7963
61a6ea1590c4f06a6966e944ebd4d81b
62d53eb2b05a3fa779ebca2d08b1d649
6a55850ea54668d98c32ffe954cd5d85
8bf81cdcfecead61b2531dcff597b133
9c9b1b98d9c7863df5905ff877767c55
a3b4868ec1671ffab6b509d62ea129ac
a6142ce837fd402ab9570ab58d46ad10
aa4561de55bdbd95702342b820910e0a
ad151215c9d7c02e6b75fe2e51f91f0b
d72ca8cd3e0e7b9f1f5dd62ca5113c8c
da3d3df2fa7d539899b27c64300807a2
e3f79edf54d590568791f77318ac0578
e95c363dc97ff58f5f22633517be6969
ee227f53a1c1e24edfa9f44c9c6a009f
f76b0363f016a0d4ec6124b844e10cff
feee13e2908e4e3d18104896d912fbf9
ffc20926598b277e509c7bf3465557eb
```

URL

```
http://103.27.185.139/icatchplugin1
http://185.183.96.139/g
http://188.209.49.219/f
http://188.209.49.244/f
http://188.209.49.244/r
http://188.209.49.244/usa
http://190.115.18.37/f
http://45.10.90.89/j
http://45.10.90.89/z
http://46.166.151.200/w
http://74.91.115.209/w
http://82.223.101.182/f
http://82.223.101.182/k
```

C2

```
lakusdvroa.com:8080                 #Chalubo
45.10.90.89:61002                   #FBot
wor.wordtheminer.com:8725           #Moobot
nlocalhost.wordtheminer.com:422     #Moobot_xor
nlocalhost.wordtheminer.com:9746    #Moobot_xor
```

IP

45.10.90.89	Ukraine	ASN48693	Rices Private
46.166.151.200	Netherlands	ASN43350	NForce Enter
74.91.115.209	United States	ASN14586	Nuclearfallou
82.223.101.182	Spain	ASN8560	1&1 Ionos Se
103.27.185.139	Japan	ASN134835	Starry Netwo
185.183.96.139	Netherlands	ASN60117	Host Sailor I
188.209.49.219	Netherlands	ASN49349	Dotsi, Unipes
188.209.49.244	Netherlands	ASN49349	Dotsi, Unipes
190.115.18.37	Belize	ASN262254	DANCOM LTD

LILIN DVR

LILIN DVR 在野0-day 漏洞分析报告

Botnet

Mozi, Another Botnet Using DHT

LILIN DVR 在野0-day 漏洞分析报告

1 post →

本文作者：马延龙，涂凌鸣，叶根深，刘宏达 当我们研究Botnet时，我们一般看到的是攻击者通过N-day漏洞植入Bot程序。但慢慢的，我们看到一个新的趋势，一些攻击者开始更多地利用0-day漏洞发起攻击，利用手段也越发成熟。我们希望安全社区关注到这一现象，积极合作共同应对0-day漏洞攻击威胁。 背景介绍 从2019年8月30号开始，360Netlab...


Mar 20, 2020 · 5 min read

Mozi Botnet relies on the DHT protocol to build a P2P network, and uses ECDSA384 and the xor algorithm to ensure the integrity and security of its components and P2P network. The sample spreads via Telnet with weak passwords and some known exploits


Dec 23, 2019 · 11 min read