

LILIN DVR

LILIN DVR 在野0-day 漏洞分析报告



Alex.Turing, Genshen Ye

Mar 20, 2020 · 5 min read

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o-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o-day漏洞攻击威胁。

背景介绍

从2019年8月30号开始，360Netlab未知威胁检测系统持续监测到多个攻击团伙使用LILIN DVR o-day漏洞传播Chalubo[1]，FBot[2]，Moobot[3]僵尸网络。

在2020年1月19号，我们开始联系设备厂商LILIN。在2020年2月13号，厂商修复了该漏洞[4]，并发布了最新的固件程序2.0b60_20200207[5]。

漏洞分析

LILIN o-day漏洞主要包括：硬编码登陆账号密码，`/z/zbin/dvr_box` 命令注入漏洞和`/z/zbin/net_html.cgi` 任意文件读取漏洞。其中`/z/zbin/dvr_box`对外提供Web服务，它的Web接口`/dvr/cmd` 或 `/cn/cmd` 存在命令注入漏洞。我们观察到被注入的参数包括：NTPUpdate，FTP，NTP。

硬编码登陆账号密码列表：

默认账号密码:

admin/123456

NTPUpdate 注入漏洞分析

1. /z/zbin/dvr_box 程序中的 `dvr_serv::do_request()` 函数负责解析 `DVRPOST` 传入的XML配置，并调用相应的处理函数；
2. `dvr_core::NTPUpdate()` 函数将Server字段传入到依赖库libutility.so中的 `UtilityBox::UtilityNtp::run()` 函数；
3. `UtilityBox::UtilityNtp::run()` 函数根据Server字段值，拼接并执行 ntp时间同步命令；
4. 由于以上过程缺乏对Server字段的特殊字符的过滤，导致命令注入。

在2.0b60_20200207版本中，厂商在步骤3通过调用

`UtilityBox::Utility::ValidateHostName()` 函数检验Server字段，修复了该漏洞。

```

1 signed int __fastcall UtilityBox::UtilityNtp::run(UtilityBox::UtilityNtp *this, const char *Server)
2 {
3     UtilityBox::Utility *v2; // r6
4     int v3; // r5
5     const char *server; // r1
6     const char *v6; // r1
7     int v7; // r5
8     int v8; // r0
9     int v9; // [sp+0h] [bp-30h]
10    char v10; // [sp+10h] [bp-20h]
11    UtilityBox::Utility *v11; // [sp+1Ch] [bp-14h]
12
13    v2 = (UtilityBox::Utility *)Server;
14    if ( !*(DWORD *)this + 34 )
15        return -1;
16    if ( !Server )
17        return -1;
18    if ( !j_strlen1((int *)Server) )
19        return -1;
20    if ( !UtilityBox::Utility::ValidateHostName(v2, server) )
21        return -1;
22    UtilityBox::UtilityString::UtilityString((UtilityBox::UtilityString *)&v10, "msntp -V -c 1 -r %s", v2);
23    v7 = UtilityBox::Utility::system(v11, v6);

```

FTP和NTP 注入漏洞分析

1. 通过硬编码登陆账号密码和 /z/zbin/net_html.cgi 程序中的任意文件读取漏洞[6]，获取设备配置文件信息 /zconf/service.xml；

2. 修改 `/zconf/service.xml` 中的FTP或NTP参数的Server字段，注入后门命令；
3. 通过硬编码账号密码远程访问 `POST /dvr/cmd` 接口，使用 `SetConfiguration` 功能，传入修改后的XML实体，向目标设备写入配置文件；
4. 设备会定时同步FTP或NTP配置，触发命令执行。

值得注意的是，FTP或NTP配置的命令注入依赖于步骤1，2获取到的网络配置信息。如果直接执行步骤3，则可能会使设备断网。

在2.0b60_20200207版本中，厂商修复了步骤1中的任意文件读取漏洞，`/z/zbin/dvr_box` 写入配置时会调用 `UtilityBox::Utility::ValidateHostName()` 函数检验Server字段，修复了步骤3中的漏洞。

```

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     }

```

时间线

2019年8月30号，发现Chalubo通过LILIN 0-day NTPUpdate漏洞进行传播。
 2020年1月11号，发现FBot通过LILIN 0-day FTP/NTP漏洞进行传播。
 2020年1月19号，第一次联系厂商，没有得到回复。
 2019年1月26号，发现Moobot通过LILIN 0-day FTP/NTP漏洞进行传播。
 2020年2月10号，第二次联系厂商，得到回复。
 2020年2月12号，向厂商提供了在野FTP和NTP漏洞PoC细节信息。
 2020年2月14号，厂商回复我们已经修复该漏洞，并发布最新的固件程序2.0b60_20200207。

受影响的固件列表

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

处置建议

我们建议LILIN DVR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，URL和域名进行监控和封锁。

联系我们

感兴趣的读者，可以在 [twitter](#) 或者在微信公众号 **36oNetlab** 上联系我们。

IoC list

样本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
fee13e2908e4e3d18104896d912fbf9
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 Enteri
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



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best Newest Oldest

Be the first to comment.

[Subscribe](#)[Privacy](#)[Do Not Sell My Data](#)

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

LILIN DVR



Multiple botnets are spreading using LILIN DVR 0-day

Icnanker

Icnanker, 一个使用了SHC技术的木马下载器

背景介绍 2019年8月15日，360Netlab恶意流量检测系统发现一个通过SSH传播的未知ELF样本(5790dedae465994d179c63782e51bac1)产生了Elknot Botnet的相关网络流量，经分析这是一个使用了"SHC(Shell script compiler)"技术的Trojan-Downloader，作者是老牌玩家icnanker。icnanker其人于2015年被网络曝光，擅长...

LILIN DVR

Multiple botnets are spreading using LILIN DVR 0-day

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....



1 post →



• Mar 23, 2020 • 9 min read



Mar 20,
2020

4 min
read