D-Link-Dir-850L-远程命令执行漏洞

janes / 2017-08-21 03:08:00 / 浏览数 4988 安全技术 漏洞分析 顶(0) 踩(0)

0x00 背景

2017年6月11日hack2Win(网络设备黑客竞赛)举办首届线上比赛，参赛选手可以通过互联网连入D-Link Dir-850L路由器然后黑掉它，其中有一名选手实现了远程任意代码执行。D-Link官方在7月27日推出了Dir-850L路由器1.47B07版本的补丁，地址:http://support.dlink.com/ProductInfo.aspx?m=DIR-850L。

现今公布了Hack2Win竞赛中提交的3个漏洞的相关细节，地址:https://blogs.securiteam.com/index.php/archives/3364。

- 通过广域网或局域网实现远程代码执行
- 通过广域网或局域网实现远程未授权信息泄露
- 通过局域网实现root用户远程代码执行

这里仅仅分析远程命令执行的漏洞。

0x01 获取源码

D-Link Dir-850L 路由器的固件可以从官方下载获取，这里下载1.14.B07版本的固件，地址: ftp://ftp2.dlink.com/PRODUCTS/DIR-850L/REVA/DIR-850L_REVA_FIRMWARE_1.14.B07_WW.ZIP。下载固件并解压后，我们得到固件文件DIR850LA1_FW114b07WW

上图可以看到该固件采用的是Squashfs文件系统，从binwalk解压出的文件中找到190090.squashfs文件，然后继续用binwalk提取，得到如下内容

可以看出这是一个标准的linux文件根目录。我们需要关注的是处理web服务的程序，该程序开启各种服务端口，并且为外部访问提供配置，修改等服务，文件存在于htdocs
其中应用层的服务是用PHP语言编写，也是本次分析需要重点关注的地方。

0x03 分析远程命令执行漏洞

要成功利用远程代码执行漏洞，需要组合未授权任意文件上传漏洞和命令注入漏洞才能实现。

未授权任意文件上传漏洞利用`hedwig.cgi`上传xml文件，获取管理员用户名和密码。当管理员接口设置改变时，会将改变的设置以xml的格式发送给`hedwig.cgi`，`hedwi`

```
foreach ($prefix."/postxml/module")
{
   del("valid");
   if (query("FATLADY")=="ignore") continue;
   $service = query("service");
   if ($service == "") continue;
   TRACE_debug("FATLADY: got service [".$service."]");
   $target = "/htdocs/phplib/fatlady/".$service.".php";
   $FATLADY_prefix = $prefix."/postxml/module:".$InDeX;
   $FATLADY_base   = $prefix."/postxml";
   if (isfile($target)==1) dophp("load", $target);
```

可以看出，`fatlady.php`直接将xml文件中的service拼接在了路径中，没有做任何校验，然后直接加载文件，加载的文件以'.php'结尾，那么可以构造service为`../../..`

读取用户名和密码。

有了用户名和密码，可以登录，然后利用NTP服务器的命令注入漏洞实现命令执行。命令注入漏洞发生在`/etc/services/DEVICE.TIME.php`文件,
核心代码如下：

```
/* NTP ... */
$enable = query("/device/time/ntp/enable");
if($enable=="") $enable = 0;
$enablev6 = query("/device/time/ntp6/enable");
if($enablev6=="") $enablev6 = 0;
$server = query("/device/time/ntp/server");
$period = query("/device/time/ntp/period"); if ($period=="") $period="604800";
$period6 = query("/device/time/ntp6/period");   if ($period6=="") $period6="604800";
$ntp_run = "/var/run/ntp_run.sh";
if ($enable==1 && $enablev6==1)
{
   if ($server=="") fwrite(a, $START, 'echo "No NTP server, disable NTP client ..." > /dev/console\n');
   else
   {
       fwrite(w, $ntp_run, '#!/bin/sh\n');
```

```
fwrite(a, $ntp_run,
    'echo "Run NTP client ..." > /dev/console\n'.
    'echo [$1] [$2] > /dev/console\n'.
    'STEP=$1\n'.
    'RESULT="Null"\n'.
    'xmldbc -s /runtime/device/ntp/state RUNNING\n'.
    'SERVER4='.$server.'\n'.
    'SERVER6=`xmldbc -g /runtime/device/ntp6/server | cut -f 1 -d " "`\n'.
    'if [ "$STEP" == "V4" ]; then\n'.
    '   xmldbc -t "ntp:'.$period.':'.$ntp_run.' $STEP"\n'.
    '   echo "ntpclient -h $SERVER4 -i 5 -s -4" > /dev/console\n'.
    '   ntpclient -h $SERVER4 -i 5 -s -4 > /dev/console\n'.
```

可以看出通过$server变量直接拼接在了命令执行的代码中，没有做任何校验，存在命令注入。那么需要构造恶意的service数据，方法同获取用户的用户名和密码方式相

根据得到的xml文件格式，构造数据发送给hedwig.cgi加载服务, 设置服务enable=1, server为恶意命令，在23090端口开启telnetd服务。

最后设置加载的服务生效，向pigwidgeon.cgi发送激活请求。

服务激活后，telnet远程连接23090端口测试。

0x04 防御方案

官方针对此次漏洞已经推出了补丁，推荐下载官方补丁更新，详情:http://support.dlink.com/ProductInfo.aspx?m=DIR-850L。或者，开启防火墙，禁止外网访问web服务

0x05 后记

针对公布的Dir-850L路由器漏洞，官方发布了相应的补丁，但是Dir系列其他的路由器是否存在同样漏洞呢？测试Dir-815路由器，发现存在相同漏洞的，然而官方并没有及时
http://support.dlink.com/ProductInfo.aspx?m=DIR-815。根据以往Dir系列爆出的漏洞来看，猜测D-Link
Dir系列多数路由器都是受该漏洞影响，建议大家开启路由器防火墙，禁止外网访问web服务或设置访问地址白名单，以此降低被黑的风险，同时多关注官方的动态和安全补

0x06 参考

- https://blogs.securiteam.com/index.php/archives/3310
- https://blogs.securiteam.com/index.php/archives/3364
- http://support.dlink.com/ProductInfo.aspx?m=DIR-850L

上一篇：- 下一篇：Burp Suite插件开发-HT...

1. 1 条回复

simeon 2017-08-23 03:01:46

牛逼的帖子，先收藏，再学习！

0 回复Ta

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板