CVE-2020-15892:Classic Stack Based Buffer Overflow in D-LINK Firmware DAP 1520

Classic Stack Based Buffer Overflow in D-LINK Firmware DAP 1520

Loginsoft-2020-1006

23 July, 2020

CVE Number

CVE-2020-15892

CWE

CWE-121: Stack-based Buffer Overflow

Product Details

The DAP-1520 Wireless AC750 Dual Band Range Extender is a portable Wireless Range Extender that lets you expand an existing wireless network's coverage area. You can place it anywhere in your home to increase the range of your wireless network. It's unobtrusive, compact design provides flexible placement and Next-generation AC750 wireless performance.

URL: https://legacy.us.dlink.com/pages/product.aspx?id=c9525c84034642bab9e2893b9b6d5134

Vulnerable Firmware Versions

1.0.8 & 1.10B04

Hardware

Ax

Vulnerability Details

A classic stack-based buffer overflow exists in D-link DAP 1520 access point, in the `ssi` binary, leading to arbitrary command execution.

SYNOPSIS

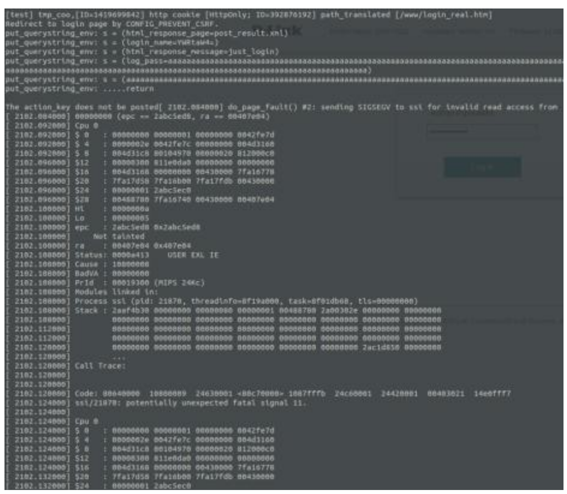
Whenever a user performs a login action from the web interface, the request values are being forwarded to the `ssi` binary. On the login page, the web interface restricts the password input field to a fixed length of 15 characters.
The problem is that validation is being done on the client-side, hence it can be bypassed when an attacker manages to intercept the login request (POST based) & tampers the vulnerable parameter (`log_pass`), to a larger length, the request will be forwarded to the webserver. The same weakness can be taken advent of in order to carry out a stack-based overflow.
Few other POST Variables, being transferred as part of the login request are also vulnerable, which are `html_response_page` & `log_user`.

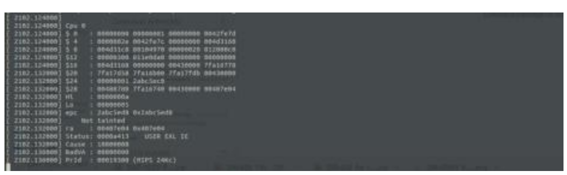
Analysis

Payload: 'a'* 256
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Request:
URL – http://192.168.0.1/apply.cgi

POST Data –
html_response_page=post_result.xml&login_name=YWRtaW4%3D&html_response_message=just_login&log_pass=$Payload&login_





Exploitation:

In a regular scenario, an attacker can be anyone connected to the network & able to access the router login page. He can inject the payload into the vulnerable fields from the web interface & perform command execution.
The attack can also be carried out remotely, by enticing the victim to visit a crafted URL, triggering the request along with the injected payload via CSRF attack.

Mitigation

- Length check should be done on the server side.
- Memory should be dynamically allocated, when the input is not trusted.

Vendor Disclosure: 9 february 2019

Credit

Discovered by ACE Team – Loginsoft

Let us know how we can help you

US Office
4437 Brookfield Corporate Drive, Suite 101
Chantilly, VA USA 20151.
+1 703 956 7410

Canada Office
7-7003 Steeles Ave W, Toronto,
ON M9W 0A2, Canada.

India Office
1-63-5-8B, Kavuri Hills, Jubilee Hills,
Hyderabad-500033.