tenable

Command Injection Vulnerability in /bin/protest Binary on Multiple D-Link Routers

Medium

← View More Research Advisories

Synopsis

Command Injection in /bin/protest

AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H (7.8/7.1)

The /bin/**protest** binary on various D-Link router firmware images is vulnerable to command injection. This allows an authenticated attacker to execute arbitrary shell commands as root, and can easily be used to obtain a root shell on the device.

In order to exploit this vulnerability, we first need to obtain access to the **/bin/cli** interface over telnet. In order to access this interface on the DIR-2640, we must first:

1. download the router's configuration binary
2. decrypt and unpack that binary using D-Link's own **mkconfig** binary, which can be found on several of their firmware images
3. set the **telnetEnabled** field in **config_2g** to **1**
4. repack and re-encrypt the config file using the same tool
5. upload the modified config through the router's web interface
6. connect to the router over telnet on port 23

We will then be prompted for a password. The password will be the one set as the admin password for the web UI followed by the suffix **@twsz2018**.

This will take us to the "**router>** " prompt.

This will launch a telnet shell, listening on port 4444, which may then be accessed without providing any further authentication.

Demonstration of Vulnerability on DIR-2640 Firmware Version 1.11B2

We have established that this vulnerability exists on the DIR-2640 router, running firmware version 1.11B2, as shown in the animated GIF below.

tenable

Those images were tested the following fashion:

1. First, the firmware image was unpacked (and decrypted, if necessary), and the root file system isolated.
2. I then checked for a binary named **protest** was found on the filesystem. If no such binary was found, then the image was ignored.
3. I would then ensure that the **cli** binary was present as well, and that the protest functionality could be triggered from the **cli** interface.
4. Using a QEMU emulator for the appropriate architecture, I executed the cli binary inside a chroot jail, restricted to the firmware image's root filesystem, under supervision by **strace**, and fed the **cli** process a payload similar to the one shown above. The injected command, however, was set to `/VULNERABLE`.
5. I then inspected the **strace** output to see if a system call beginning with `execve("/VULNERABLE"` had taken place. If it had, this meant that command injection was possible on that build of protest, exposed through the **cli** interface.

Disclosure Timeline

December 28, 2021: Vendor notified
December 28, 2021: Vendor responds, requesting further details
December 28, 2021: Tenable responds to vendor, with additional details
December 28, 2021: Issue forwarded to vendor's R&D department
February 7, 2022: Tenable contacts vendor with additional information
February 8, 2022: Vendor acknowledges

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: CVE-2022-1262

CVSSv3 Vector: AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Additional Keywords : router
command injection

Affected Products:

DIR-1360 A1 firmware version 1.02B03
DIR-1360 A1 firmware version 1.03B02
DIR-1360 A1 firmware version 1.11B04
DIR-1360 firmware version 1.00B15
DIR-1360 firmware version 1.01B03
DIR-1360 firmware version 1.11B04 Beta for WPA2 2020/11/03
DIR-1760 firmware version 1.01B04
DIR-1760 firmware version 1.11B03 Beta for WPA2 2020/11/03
DIR-1960 A1 firmware version 1.02B01
DIR-1960 A1 firmware version 1.03B03
DIR-1960 A1 firmware version 1.11B03
DIR-1960 firmware version 1.11B03 Beta for WPA2 2020/11/03
DIR-2640 A1 firmware version 1.01B04
DIR-2640 A1 firmware version 1.11B02
DIR-2640 firmware version 1.11B02 Beta for WPA2 2020/11/03
DIR-2660 A1 firmware version 1.04B03
DIR-2660 A1 firmware version 1.11B04
DIR-2660 firmware version 1.00B14
DIR-2660 firmware version 1.01B03
DIR-2660 firmware version 1.02B01
DIR-2660 firmware version 1.03B04
DIR-2660 firmware version 1.11B04 Beta for WPA2 2020/11/03
DIR-3040 A1 firmware version 1.11B02
DIR-3040 A1 firmware version 1.12B01
DIR-3040 A1 firmware version 1.13B03
DIR-3040 A1 firmware version 1.20B03
DIR-3040 firmware version 1.13B03 Beta for WPA2 2020/11/03
DIR-3060 A1 firmware version 1.01B07
DIR-3060 A1 firmware version 1.02B03
DIR-3060 A1 firmware version 1.11B02 Beta for Guest zone connect issue 2020/01/19
DIR-3060 A1 firmware version 1.11B04
DIR-3060 firmware version 1.00B12
DIR-3060 firmware version 1.11B04 Beta for WPA2 2020/11/03

DIR-878 firmware version 1.30B08
DIR-882 A1 firmware version 1.30B06
DIR-882 A1 firmware version 1.30B10
DIR-882 firmware version 1.20B06
Risk Factor: Medium

Advisory Timeline

April 6, 2022: Advisory Published

tenable

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media