Talos Vulnerability Report

TALOS-2020-1065

Synology SRM lbd service Command Execution Vulnerability

OCTOBER 29, 2020

CVE NUMBER

CVE-2020-27654, CVE-2020-11117

Summary

An exploitable command execution vulnerability exists in the lbd service functionality of Qualcomm lbd 1.1, as present in Synology SRM 1.2.3 RT2600ac 8017-5. A specially crafted debug command can overwrite arbitrary files with controllable content, resulting in remote code execution. An attacker can send an unauthenticated message to trigger this vulnerability.

Tested Versions

Qualcomm lbd 1.1
Synology SRM 1.2.3 RT2600ac 8017-5

Product URLs

https://www.synology.com/en-global/srm

CVSSv3 Score

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

CWE

CWE-73 - External Control of File Name or Path

Details

Synology Router Manager (SRM) is a Linux-based operating system for Synology Routers developed by Synology.

SRM ships a binary called “Qualcomm Load Balancing Daemon” (`lbd`), which is used for monitoring and debugging a load-balancing feature in the WiFi interfaces. This service can be managed via network, and there are two instances of it running at the same time, one for the main WiFi (port 7787) and one for the guest WiFi (port 7786). The two instances are configured in the exact same way, except for the interface they manage. Both ports are reachable via LAN.

The service has no authentication and shows a menu:

```
$ nc 192.168.1.1 7786
Use `h' and `help' for help messages
Use `dbg here' to see log messages; other dbg cmds for log level
@
```

In the `dbg` menu, there’s an option to “redirect” debug output to a file.

```
@ dbg h
h [cmd] -- short help (first line of each help message).
help [cmd] -- long help.
q -- quit interactive menu
s -- print dbg status
level [{<module>|all} [[=] {err|info|debug|dump}] -- print/change module debug level
here [-off] -- copy debug messages to current shell context
redirect {[-a] <path>} | -off -- redirect dbg messages to file
```

An attacker could connect to this port, enable debug output to a file, and influence it in a way that interpretable output gets written to executable files, in order to execute arbitrary code without authentication. Any command executed this way would be run as the root user:

```
SynologyRouter> ps |grep [l]bd
29380 root      3032 S    /usr/sbin/lbd -C /usr/syno/etc/wifi/lbd.conf -P 7787
29997 root      3036 S    /usr/sbin/lbd -C /usr/syno/etc/wifi/lbd.guest.conf -P 7786
```

Note that, while this service is normally reachable only within LAN, because of the issues described in TALOS-2020-1064 and TALOS-2020-1066, this service is exploitable also from the QuickConnect network, allowing a non-authenticated attacker to execute arbitrary code as root in any device connected to the QuickConnect VPN.

Timeline

2020-05-04 - Vendor disclosure to Synology and Qualcomm
2020-06-02 - Disclosure release deadline requested and Talos extended to 2020-09-30
2020-06-22 - 2nd extension requested; disclosure extended to 2020-10-30

2020-07-09 - Vendor (Qualcomm) assigned CVE-2020-11117
2020-08-28 - Vendor (Qualcomm) confirmed patch
2020-10-29 - Public Release

CREDIT

Discovered by Claudio Bozzato of Cisco Talos.
