Talos Vulnerability Report

TALOS-2020-1066

Synology SRM QuickConnect iptables network misconfiguration vulnerability

OCTOBER 29, 2020

CVE NUMBER

CVE-2020-27655

Summary

An exploitable network misconfiguration vulnerability exists in the QuickConnect iptables functionality of Synology SRM 1.2.3 RT2600ac 8017-5. Packets originating from the QuickConnect VPN interface are not filtered, resulting in unrestricted communication with any network service running in the device.

Tested Versions

Synology SRM 1.2.3 RT2600ac 8017-5

Product URLs

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

CVSSv3 Score

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

CWE

CWE-284 - Improper Access Control

Details

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

SRM has a feature called QuickConnect, which allows users to remotely manage their router. This feature requires a Synology account and users have to set it up from the router Web interface in order to use it. The setup also requires the user to choose an arbitrary “QuickConnect ID”, which will be used as a remote identifier for the router.

Once activated, the user is presented with a link that can be used to connect from anywhere via a browser, example: “http://QuickConnect.to/qcrouterid”, where “qcrouterid” is the previously chosen identifier. When browsing this link, the router is instructed (via a previously-established channel between router and Synology servers) to establish a VPN connection with the remote QuickConnect endpoint. At this point, requests performed by the browser will be relayed to the internal router Web interface on port 8001 by default (SSL).

The VPN connection is established using OpenVPN in client mode. Once connected, the router gets an IP address for a subnet in the 169.254.0.0/16 network:

```
SynologyRouter> ip addr
...
36: tun1000: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1400 qdisc fq_codel state UNKNOWN group default qlen 100
link/none
inet 169.254.171.94/21 brd 169.254.175.255 scope global tun1000
   valid_lft forever preferred_lft forever
...
```

As demonstrated in TALOS-2020-1064, an attacker could manage to communicate with any device connected to the VPN.

From the QuickConnect configuration page in the SRM router (and possibly any other Synology device having this feature), it’s possible to select which service to enable in the VPN: SRM, File Sharing, Mobile Applications (DS get, DS file, DS router).

However, in the bare VPN channel, it’s not only possible to communicate with the device’s web interface, but also to any local service, despite what has been configured by the user.

This is because of a misconfiguration in iptables rules:

```
SynologyRouter> iptables -L -v -n
Chain INPUT (policy ACCEPT 2 packets, 140 bytes)
 pkts bytes target              prot opt in     out     source               destination
 1745  320K QUICKCONN_INPUT     all  --  *      *       0.0.0.0/0            0.0.0.0/0       [1]
    2   140 INPUT_FIREWALL      all  --  *      *       0.0.0.0/0            0.0.0.0/0
 1671  149K URL_BLOCKER_FILTER  all  --  *      *       0.0.0.0/0            0.0.0.0/0
 1990  213K ULOGD_DHCP_INPUT    all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain QUICKCONN_INPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
  851  135K ACCEPT     all  --  tun1000 *      0.0.0.0/0            0.0.0.0/0            [2]
```

As we can see in [1] and [2], any packet coming from the tun1000 interface (QuickConnect VPN) is accepted without filtering.

By exploiting this issue together with TALOS-2020-1064, a non-authenticated attacker would be able remotely communicate with any device connected to the QuickConnect VPN without any kind restriction, in order to execute additional attacks.
For example, it would be possible to exploit TALOS-2020-1065 in order to execute arbitrary commands as the root user.

Note that an attacker could enter the QuickConnect VPN either by simply owning a router and connecting to it via SSH, or, alternatively, using the bug described in TALOS-2020-1058.

Timeline

2020-05-04 - Vendor disclosure
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
2020-10-29 - Public Release

CREDIT

Discovered by Claudio Bozzato of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1065

NEXT REPORT TALOS-2020-1058

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.