Talos Vulnerability Report

TALOS-2020-1061

Synology SRM QuickConnect HTTP connection Information Disclosure Vulnerability

OCTOBER 29, 2020

CVE NUMBER

CVE-2020-27653

SUMMARY

An exploitable information disclosure vulnerability exists in the QuickConnect HTTP connection functionality of Synology SRM 1.2.3 RT2600ac 8017-5. An attacker can impersonate the remote VPN endpoint in order to downgrade the HTTPS connection to HTTP, allowing an attacker to capture the web interface communication and in turn steal the session cookies. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.

CONFIRMED VULNERABLE VERSIONS

The versions below were either tested or verified to be vulnerable by Talos or confirmed to be vulnerable by the vendor.

Synology SRM 1.2.3 RT2600ac 8017-5
Synology DSM 6.2.3 25426 (confirmed by vendor)

PRODUCT URLS

SRM - https://www.synology.com/en-global/srm DSM - https://www.synology.com/en-global/dsm

CVSSV3 SCORE

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

CWE

CWE-757 - Selection of Less-Secure Algorithm During Negotiation (‘Algorithm Downgrade’)

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, in particular this is the command line command which is executed by the device:

```
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 /usr/syno/etc/synorelayd/ca/ca.crt \
  --script-security 2 --auth-user-pass /tmp/.tunnel.[id] --remap-usr1 SIGTERM \
  --cipher none --comp-lzo adaptive --reneg-sec 0 --verb 0 \                        # [1]
  --route-up "/usr/syno/etc.defaults/synorelayd/scripts/up.sh 32317" \
  --down /usr/syno/etc.defaults/synorelayd/scripts/down.sh \
  --syno-no-verify \
  --allow-recursive-routing
```

Note at [1] the command line option “–cipher none”, meaning that VPN data channel packets are not encrypted. This means that an attacker that can perform a man-in-the-middle attack between the router and the remote QuickConnect servers, can capture plaintext traffic.
However, the SRM web interface is normally exposed via QuickConnect via HTTPS by default, so an attacker that solely captures the VPN traffic won’t be able to access the plaintext content of the HTTPS connection.

Despite this, an attacker can downgrade the HTTPS connection inside the VPN to HTTP. The steps to pursue such an attack are the following:

1. redirect all connections towards [quickconnect]:443 to the attacker machine [attacker]
2. redirect the traffic from [attacker]:443 to a local (fake) OpenVPN server (e.g. [attacker]:1194)
3. start the OpenVPN server:

```
/usr/bin/openvpn --mode server --tls-server --proto udp --port 1195 \
    --dev tun --ca customca.crt --cert customcrt.crt --key customcrt.key \
    --dh dh.pem --verb 2 --cipher none --auth none --verify-client-cert none \
    --auth-user-pass-verify /bin/true via-file --script-security 2
```

4. the end-user tries to connect to its router remotely, by browsing “http://QuickConnect.to/qcrouterid”

5. the router connects to the fake OpenVPN server, but this connection immediately terminates because of an invalid certificate
6. redirect the traffic from [attacker]:443 to the legitimate QuickConnect server ([quickconnect]:443)
7. the router will retry to establish the VPN connection. This time the connection reaches the QuickConnect servers and will be established
8. the browser now contacts the QuickConnect servers via HTTP rather than HTTPS.

The reason for this is a previous request to “https://dec.quickconnect.to/Serv.php”:

```
- Request
Request URL:https://dec.quickconnect.to/Serv.php
Request Method:POST
Remote Address:52.58.180.63:443

[{"version":1,"command":"request_tunnel","stop_when_error":false,"stop_when_success":true,"id":"dsm_portal_https","serverID":"qcrouterid","i
s_gofile":false},
{"version":1,"command":"request_tunnel","stop_when_error":false,"stop_when_success":true,"id":"dsm_portal","serverID":"qcrouterid","is_gofil
e":false}]

- Answer
[
{
    "command": "request_tunnel",
    "errinfo": "request_tunnel.go:193[tunnel request fail]",
    "errno": 8,
    "version": 1
},
{
    "command": "request_tunnel",
    "env": {
        "control_host": "dec.quickconnect.to",
        "relay_region": "de7"
    },
    "errno": 0,
    "server": {
        "ddns": "...",
        "ds_state": "CONNECTED",
        "external": {
            "ip": "...",
            "ipv6": "::"
        },
        "fqdn": "NULL",
        "gateway": "...",
        "interface": [...]
        "ipv6_tunnel": [],
        "serverID": "...",
        "tcp_punch_port": 0,
        "udp_punch_port": 36668,
        "version": "8017"
    },
    "service": {
        "ext_port": 0,
        "https_ip": "185.102.219.105",
        "https_port": 443,
        "pingpong": "DISCONNECTED",
        "pingpong_desc": [],
        "port": 8000,
        "relay_dn": "der7.re.cs.quickconnect.to",
        "relay_dualstack": "derds7.re.cs.quickconnect.to",
        "relay_ip": "185.102.219.105",
        "relay_ipv6": "2a02:6ea0:c704::1:105",
        "relay_port": 30141
    },
    "version": 1
}
]
```

The request above shows the results of two “commands”: the first happening via HTTPS which failed, and a second one happening via HTTP (notice port 8000), which succeded. At this point the browser requests the router’s login page via the URL “http://qcrouterid.de7.quickconnect.to/”, that is without SSL.

The same issue happens even if the end-user connects to the router directly via a previously-generated URL (e.g. via page refresh), but in this case a “location” header is returned.

```
- Request
URL:https://qcrouterid.de7.quickconnect.to/webman/index.cgi
Request Method:GET
Remote Address:185.102.219.105:443

Host: qcrouterid.de7.quickconnect.to
User-Agent: ...
Accept: ...
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: id=0MbPP7B2zO0cs188OQ3E112233; type=tunnel; _ga=GA1.2.772635491.772635491; _gid=GA1.2.772635491.772635491;
_gat_gtag_UA_772635491_3=1
Upgrade-Insecure-Requests: 1

- Answer:
HTTP/2 307 Temporary Redirect
access-control-allow-origin: *
connetion: close
location: http://qcrouterid.de7.quickconnect.to/webman/index.cgi
strict-transport-security: max-age=0; includeSubDomains
content-length: 0
```

In both cases, when the connection is switched over HTTP, the whole data exchanged with the router’s web interface is plaintext both between router and QuickConnect servers (because of the “–cipher none” flag) and between QuickConnect servers to end-user. An attacker could capture the session cookie and use it to log into the router via QuickConnect servers.

Note that this issue is exploitable when both options “redirect HTTP to HTTPS” and “Enable HSTS” are disabled in the router (default configuration).

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-2020-1060

NEXT REPORT TALOS-2020-1064
