Talos Vulnerability Report

# Synology QuickConnect servers HTTP redirection Information Disclosure Vulnerability

## CVE NUMBER

CVE-2021-26564, CVE-2021-26565, CVE-2021-26566

## Summary

An exploitable information disclosure vulnerability exists in the HTTP redirection functionality of Synology QuickConnect servers. An attacker can impersonate the remote QuickConnect servers in order to impersonate the remote device and in turn steal the device's credentials. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.

## Tested Versions

Synology QuickConnect servers

## Product URLs

https://quickconnect.to

## 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 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.

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 device is instructed (via a previously-established channel between device 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 device Web interface on port 8001 by default (SSL).

The QuickConnect link, as provided by the device web interface, uses the "http" protocol, meaning that if an end-user was to use this link to connect to its device, a classic man-in-the-middle attack could be used to steal credentials.
Moreover, even if the end-user decided to change the link into "https", the connection would be redirected to "http" [1]:

```
$ curl -v "https://QuickConnect.to/qcrouterid"
*   Trying 52.58.180.63...
* TCP_NODELAY set
* Connected to QuickConnect.to (52.58.180.63) port 443 (#0)
...
> GET /qcrouterid HTTP/2
> Host: QuickConnect.to
> User-Agent: curl/7.64.1
> Accept: */*
>
* Connection state changed (MAX_CONCURRENT_STREAMS == 128)!
< HTTP/2 302
< content-type: text/html
< content-length: 138
< location: http://qcrouterid.quickconnect.to/https_first          [1]
< server: nginx
<
<html>
<head><title>302 Found</title></head>
<body>
<center><h1>302 Found</h1></center>
<hr><center>nginx</center>
</body>
</html>
* Connection #0 to host QuickConnect.to left intact
* Closing connection 0
```

Note that the severity of this issue gets aggravated by the bug described in TALOS-2020-1059. By exploiting both bugs together, an attacker can force the user's browser to provide a valid cookie via the unencrypted HTTP connection.

## Timeline

2020-04-29 - Vendor Disclosure
2021-02-25 - Vendor Patched

## CREDIT

Discovered by Claudio Bozzato of Cisco Talos.