Talos Vulnerability Report

TALOS-2020-1059

Synology SRM web interface session cookie secure flag Information Disclosure Vulnerability

OCTOBER 29, 2020

CVE NUMBER

CVE-2020-27651

SUMMARY

An exploitable information disclosure vulnerability exists in the web interface session cookie functionality of Synology SRM 1.2.3 RT2600ac 8017-5. An attacker can impersonate the remote QuickConnect servers in order to steal a session cookie that doesn’t have the secure flag set, and in turn access the router remotely. 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-614 - Sensitive Cookie in HTTPS Session Without ‘Secure’ Attribute

DETAILS

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

SRM has a web interface that is used for management, accessible on port 8000 (HTTP) and 8001 (HTTPS).
After a successful login, the web server sets a session cookie “id”. The cookie however has no flags. This is true also when both options “redirect HTTP to HTTPS” and “Enable HSTS” are enabled in the router.

When sending the POST request for login (`https://10.3.3.78:8001/webman/login.cgi`), the answer is the following:

```
HTTP/1.1 200 OK
Server: Apache
X-SYNO-TOKEN: fl2EPyTQq0PlU
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Set-Cookie: id=flNg0ZgTre90A1920W1N933211;path=/                                 [1]
Strict-Transport-Security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 107
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset="UTF-8"
Content-Security-Policy-Report-Only: worker-src 'none'; report-uri about:blank
```

Because of the lack of “secure” flag for the cookie [1], an attacker can steal the “id” cookie (e.g. via a man-in-the-middle attack) the page, which is equivalent to having credentials to access the router.

Note that the severity of this issue gets aggravated by the bug described in TALOS-2020-1060. By exploiting both bugs together, an attacker can force the user’s browser to provide a valid cookie via an unencrypted remote HTTP connection, when using the QuickConnect feature.

TIMELINE

2020-04-29 - 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-2020-1007

NEXT REPORT

TALOS-2020-1060