Talos Vulnerability Report

TALOS-2020-1086

Synology SRM web interface session cookie HttpOnly flag information disclosure vulnerability

OCTOBER 30, 2020

CVE NUMBER

CVE-2020-27658

SUMMARY

An exploitable information disclosure vulnerability exists in the web interface session cookie functionality of Synology SRM 1.2.3 RT2600ac 8017-5. The session cookie misses the HttpOnly flag, making it accessible via JavaScript and thus allowing an attacker to perform an XSS attack and steal the session cookie.

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

PRODUCT URLS

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

CVSSV3 SCORE

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

CWE

CWE-1004 - Sensitive Cookie Without 'HttpOnly' Flag

DETAILS

Synology Router Manager (SRM) is a Linux-based operating system for Synology routers.

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 set.

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
Date: Fri, 15 May 2020 14:11:21 GMT
Server: Apache
X-SYNO-TOKEN: yG4izPeht.KUA
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Set-Cookie: id=flNg0ZgTre90A1920W1N933211;path=/                              [1]
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"

<div id='synology'>{
   "SynoToken" : "yG2yaPrht.KKA",
   "result" : "success",
   "success" : true
}
</div>
```

Because of the lack of the "HTTPOnly" flag for the "id" cookie [1], an attacker able to inject arbitrary Javascript in a page, would be able to steal the "id" cookie. This cookie can then be used, in the worst case, to login to the management interface as administrator.

As an example, in TALOS-2020-1087 we showed how it's possible to inject arbitrary Javascript and steal the "id" cookie because of the issue described here.

TIMELINE

2020-05-19 - 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.