Talos Vulnerability Report

TALOS-2020-1071

Synology SRM dnsExit DDNS provider information disclosure vulnerability

OCTOBER 29, 2020

CVE NUMBER

CVE-2020-27656-CVE-2020-27657

Summary

An information disclosure vulnerability exists in the dnsExit DDNS provider functionality of Synology SRM 1.2.3 RT2600ac 8017-5. A specially crafted man-in-the-middle attack can steal the dnsExit credentials to take over the registered subdomain. An attacker can impersonate the remote dnsExit servers to trigger this vulnerability.

Tested Versions

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

Product URLs

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

CVSSv3 Score

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

CWE

CWE-319 - Cleartext Transmission of Sensitive Information

Details

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

SRM supports DDNS (Dynamic DNS) for Synology’s DDNS and a set of third-party providers. This feature allows a user to assign a DNS entry to their public IP address, in order to serve content remotely.

One of the third-party providers supported is dnsExit.
When this provider is used, the IP address update is performed by `/usr/syno/bin/ddns/dnsexit.php`:

```
#!/usr/bin/php -d open_basedir=/usr/syno/bin/ddns
<?php

if ($argc !== 5) {
    echo 'badparam';
    exit();
}

$account = (string)$argv[1];
$pwd = (string)$argv[2];
$hostname = (string)$argv[3];
$ip = (string)$argv[4];

// check the hostname contains '.'
if (strpos($hostname, '.') === false) {
    echo 'badparam';
    exit();
}

// only for IPv4 format
if (!filter_var($ip, FILTER_VALIDATE_IP, FILTER_FLAG_IPV4)) {
    echo "badparam";
    exit();
}

// [1]
$url = 'http://update.dnsexit.com/RemoteUpdate.sv?login='.$account.'&password='.$pwd.'&host='.$hostname.'&myip='.$ip;

$req = curl_init();
curl_setopt($req, CURLOPT_URL, $url);
$res = curl_exec($req);
curl_close($req);
```

At [1] we can see that the request is performed over `http` rather than `https`, allowing an attacker to perform a man-in-the-middle attack and steal the dnsExit credentials.

Timeline

2020-05-12 - 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-2020-1058

NEXT REPORT

TALOS-2020-1086