Talos Vulnerability Report

TALOS-2020-1159

Synology DSM synoagentregisterd server finder out-of-bounds write vulnerability

APRIL 19, 2021

CVE NUMBER

CVE-2021-26560, CVE-2021-26561, CVE-2021-26562

Summary

An out-of-bounds write vulnerability exists in the synoagentregisterd server finder functionality of Synology DSM 6.2.3 25426 DS120j. A specially crafted HTTP response can lead to remote code execution. An attacker can use man-in-the-middle techniques to trigger this vulnerability.

Tested Versions

Synology DSM 6.2.3 25426-2 DS120j

Product URLs

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

CVSSv3 Score

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

CWE

CWE-121 - Stack-based Buffer Overflow

Details

Synology DiskStation Manager (DSM) is the Linux-based operating system for every Synology NAS.

Synology DSM runs a service called `synoagentregisterd`, whose task is to manage the registration of the device's local network IP address with remote Synology servers.

The service is actually a symlink to the `synosearchagent` binary, which changes its behavior depending on `argv[0]`:

```
# ls -l /usr/syno/sbin/synoagentregisterd
lrwxrwxrwx 1 root root 29 Sep 22 13:18 /usr/syno/sbin/synoagentregisterd -> /usr/syno/bin/synosearchagent
```

In order for `synoagentregisterd` to register the device's IP address, it first asks `global.quickconnect.to` for a server to reach out:

```
GET /finder/server HTTP/1.1
Host: global.quickconnect.to
User-Agent: synology_armada37xx_ds120j DSM6.2-25426 Update 2 (synoagentregisterd_dsm)
Accept: */*

HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Content-Length: 36
Connection: close
Server: nginx

syno_finder_site=dec.quickconnect.to          [1]
```

Then, it connects to the `syno_finder_site` specified in the response [1], and communicates its IP addresses (both IPv4 and IPv6):

```
GET /finder/set.php?token=somesynotoken&serial=someserial&ipv4=10.3.3.2&ipv6=ipv6addr&port=5000&https_port=5001 HTTP/1.1
Host: dec.quickconnect.to
User-Agent: synology_armada37xx_ds120j DSM6.2-25426 Update 2 (synoagentregisterd_dsm)
Accept: */*

HTTP/1.1 200 OK
Date: Tue, 22 Sep 2020 16:46:41 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 28
Connection: close
Server: nginx

{"errno":0,"interval":22800}
```

Both requests are sent in plaintext (over HTTP port 80), and can thus be easily modified by an attacker able to man-in-the-middle the connection.

In particular, the function that parses the `/finder/server` response data [1] is at `0x404248` in the `synosearchagent` binary:

```
undefined8 FUN_00404248(undefined8 param_1,char *param_2,int param_3)
{
  int iVar1;
  char *__format;
  undefined8 uVar2;
  undefined8 uVar3;
  longlong lVar4;
  longlong lVar5;
  longlong local_918;
  void *curl_writedata;
  undefined8 local_908;
  char acStack2304 [128];
  char local_880 [128];                                                    // [6]
  char url [2048];

  memset(url,0,0x800);
  memset(acStack2304,0,0x80);
  memset(local_880,0,0x80);
  ...
  snprintf(url,0x800,"http://%s/finder/server",param_1);                   // [2]
  if (DAT_00418468 != 0) {
    fprintf(stderr,"%s:%d Get finder site: [Url: %s, UserAgent: %s]\n","synoagentregisterd.c",0x171,
            url,&DAT_004183e8);
  }
  curl_writedata = malloc(0x400);
  ...
        curl_easy_setopt(lVar4,0x2712,url);                                // [3]
        curl_easy_setopt(lVar4,0x2727,lVar5);
        curl_easy_setopt(lVar4,0x2722,&DAT_004183e8);
        curl_easy_setopt(lVar4,0x34,1);
        curl_easy_setopt(lVar4,0x3e9,1);
        curl_easy_setopt(lVar4,0x4e,0xf);
        curl_easy_setopt(lVar4,0xd,0x1e);
        curl_easy_setopt(lVar4,0x4e2b,curl_write_callback);
        curl_easy_setopt(lVar4,0x2711,&curl_writedata);                    // [4]
        iVar1 = curl_easy_perform(lVar4);
        if (iVar1 == 0) {
          curl_easy_getinfo(lVar4,0x200002,&local_918);
          ...
          iVar1 = __isoc99_sscanf(curl_writedata,"syno_finder_site=%s",local_880);   // [5]
          ...
```

At [2], the `/finder/server` URL is created, which is then passed to `libcurl` [3] along with other options. Among those options we can notice `CURLOPT_WRITEDATA` [4], which is where the HTTP response data is going to be stored.
At [5] the data in `curl_writedata` is parsed and the result stored in the local stack variable `local_880`, which has a size of 128 bytes [6], without any length constraints.

An attacker able to impersonate the remote `global.quickconnect.to` server (for example using a man-in-the-middle attack, via ARP or DNS poisoning), could inject an arbitrarily long domain at [1], which will write out-of-bounds on the stack [5], possibly leading to arbitrary code execution.

Note that, while `synoagentregisterd` runs as UID 0 (root), DSM uses AppArmor to restrict applications' capabilities. However, as demonstrated in TALOS-2020-1158, it is possible to bypass the AppArmor profile for `synoagentregisterd` and gain unrestricted root access.

Timeline

2020-09-28 - Vendor Disclosure
2021-02-26 - Vendor Patched

CREDIT

Discovered by Claudio Bozzato and Lilith >_> of Cisco Talos.
