TRACK 1

HITB SECCONF
AMSTERDAM - 2021

A Journey into Synology NAS

Qian Chen (@cq674350529)

About me

- Senior Security Engineer of Qihoo 360 Nirvan Team
- Mainly focus on the security of embedded devices
- 280+ vulnerabilities (Cisco, Synology, MikroTik, Ubiquiti, DrayTek, Zyxel, TRENDnet, NETGEAR, etc.)
- Speaker of POC2019

Agenda

Introduction

Set Up

Bug Hunting

Summary

Introduction

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

Hard Disk

?

Cloud

Why Synology NAS ?

- Best seller in Amazon
- A longtime “leader in the small-business and home NAS arena”
- One of targets in Pwn2Own Tokyo 2020

Synology NAS

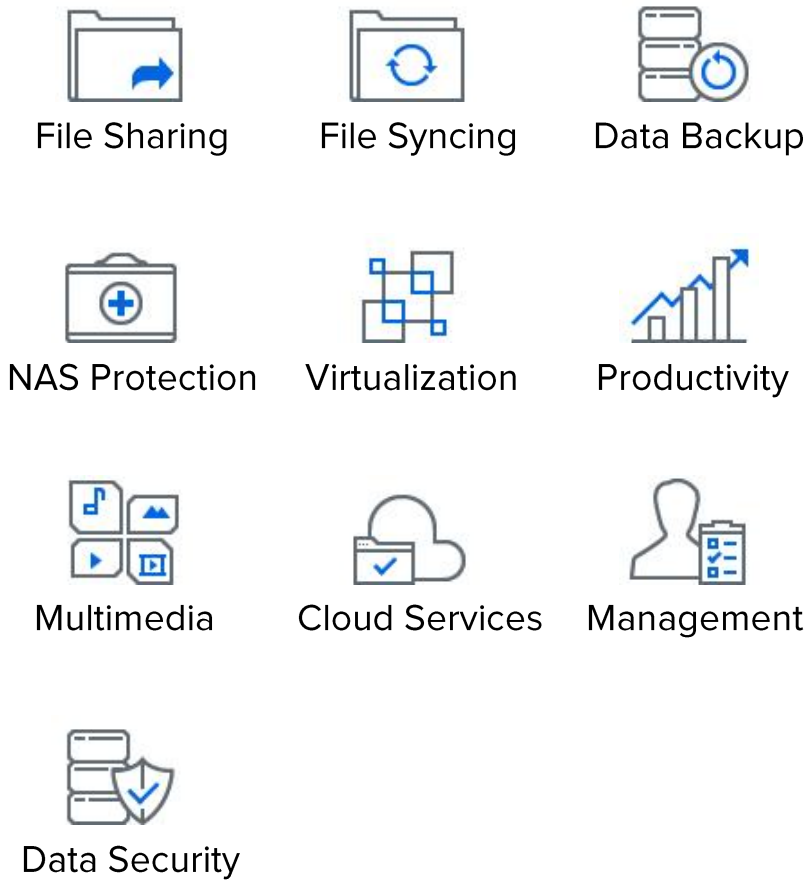
- Main product line of NAS
  - DiskStation for desktop models
  - FlashStation for all-flash models
  - RackStation for rack-mount models
- NAS models

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

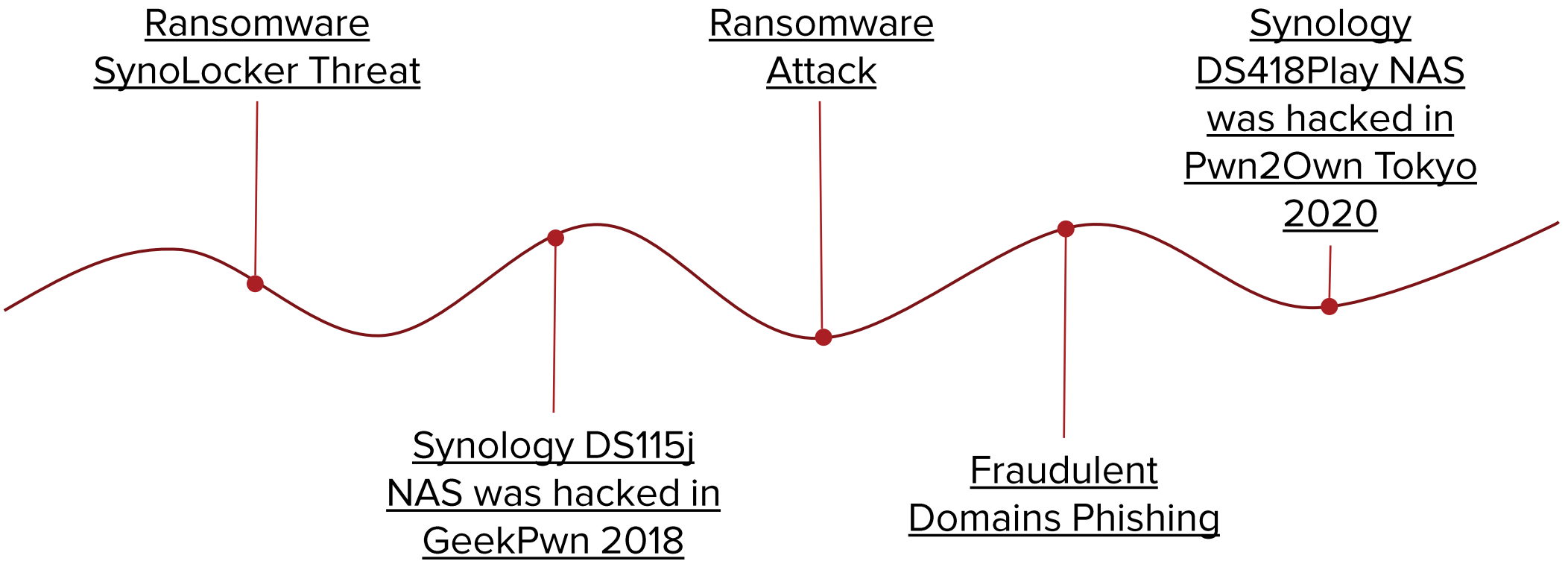
J series	Value series	Plus series
		
XS+/XS series	**SA series**	**FS series**
		

Synology DiskStation Manager(DSM)

- A Linux based software package that is the operating system for every Synology NAS.
- It’s web-based and designed to help you manage your digital assets across home and office



Synology NAS News



Previous Research

- Network Attached Security: Attacking a Synology NAS (by NCC Group)
  https://www.nccgroup.com/ae/about-us/newsroom-and-events/blogs/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/casestudies/sohopelessly-broken-2-0/index.html

- Vulnerability Spotlight: Multiple vulnerabilities in Synology SRM (Synology Router Manager) (by Cisco Talos)
  https://blog.talosintelligence.com/2020/10/vulnerability-spotlight-multiple.html

- Vulnerability Spotlight: Multiple vulnerabilities in Synology DiskStation Manager (by Cisco Talos)
  https://blog.talosintelligence.com/2021/04/vuln-spotlight-synology-dsm.html

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

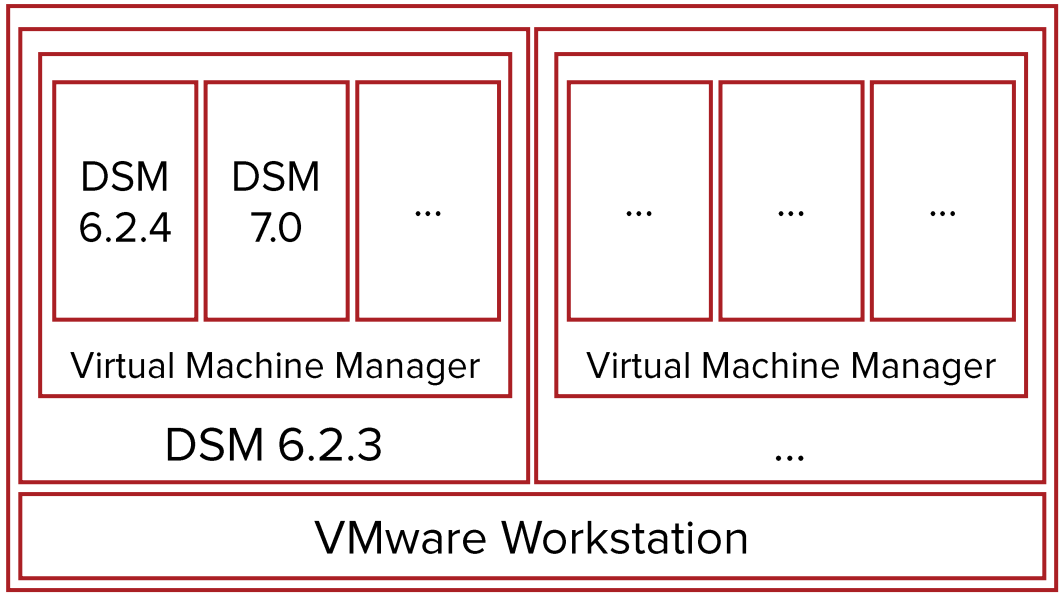
- NAS virtual machine
  - The official PAT file provided by the Synology vendor
  - An UEFI/BIOS loader
- Setup the device
  - Web Assistant: communicate via 5000/tcp
  - Synology Assistant: communicate via 9999/udp (or 9998/udp, 9997/udp)

Have trouble installing DSM 6.2.4 or DSM 7.0

- 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

Installation – "Black" Synology

- Virtual Machine Manager
  - integrate various virtualization solutions in a centralized and refined interface, allowing you to easily create, run, and manage multiple virtual machines on your Synology NAS

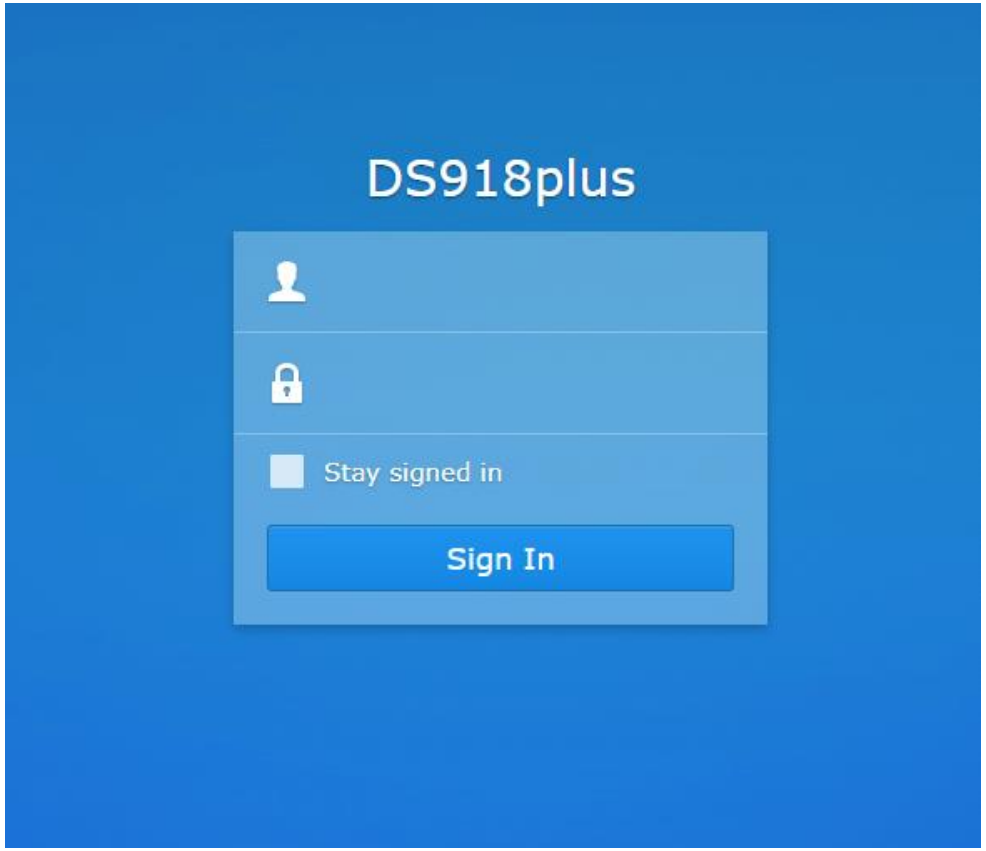


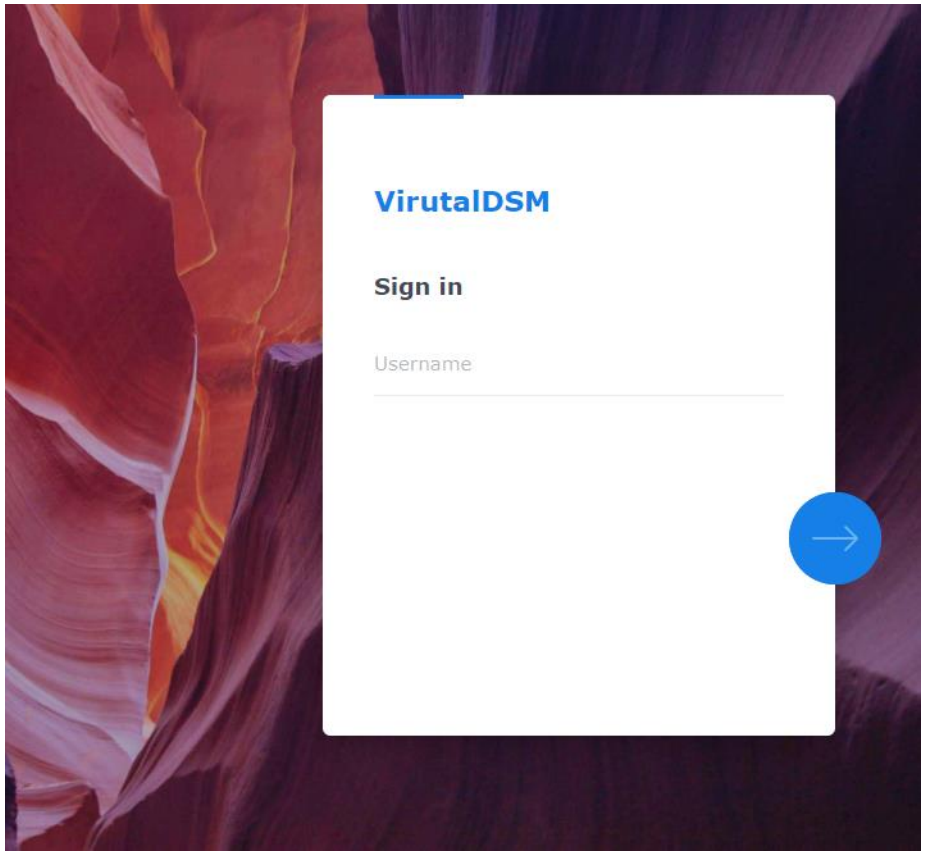
We can install another virtual DSM 6.2.4 or DSM 7.0 in a DSM instance

Docker package is a lightweight virtualization application, which can run virtual DSM as well. However, Docker DSM reached End-Of-Life on December 31, 2019

Installation – "Black" Synology

Mainly focus on DSM 6.1/6.2

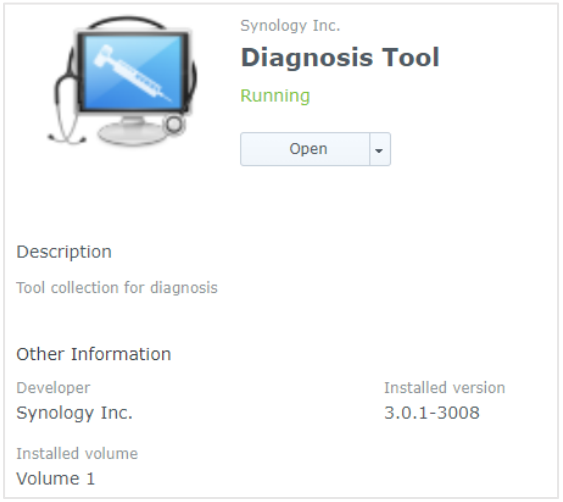




- Official DSM Online Demo: https://demo.synology.com/en-global/dsm

Preparation

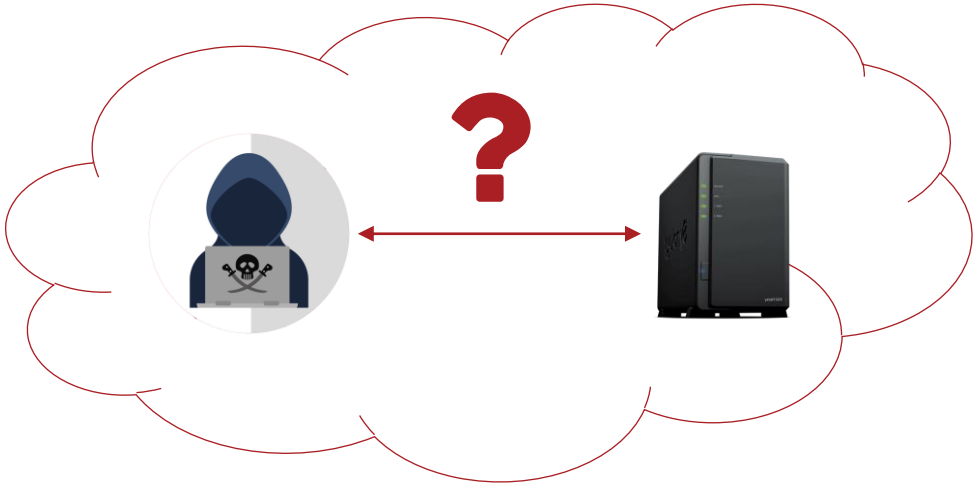
- Access to shell
  - SSH
- Install binutils: to analyze and debug the programs on device easily
  - Diagnosis tool: tool collection for diagnosis
  - Shell command: synogear install




```
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               genrio            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

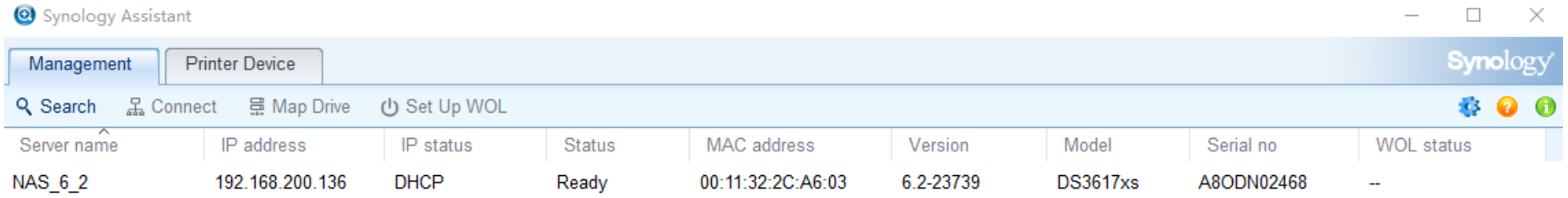
- Common services
  - smbd
  - nginx
  - ntpd
  - minissdpd
  - dhclient
  - nmbd
  - snmpd
- Custom services
  - findhostd
  - iscsi_snapshot_comm_core
  - synosnmpcd

```
root@DS918plus:~# netstat -lnp -4
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:2379          0.0.0.0:*               LISTEN      16205/etcd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      5161/smbd
tcp        0      0 127.0.0.1:2380          0.0.0.0:*               LISTEN      16205/etcd
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN      13071/sshd
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      14850/nginx: master
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      14726/postgres
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      14850/nginx: master
tcp        0      0 192.168.200.144:3260    0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:30300         0.0.0.0:*               LISTEN      16491/synovncrelayd
tcp        0      0 127.0.0.1:4700          0.0.0.0:*               LISTEN      14449/cnid_metad
tcp        0      0 127.0.0.1:16509         0.0.0.0:*               LISTEN      16446/libvirtd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      5161/smbd
tcp        0      0 0.0.0.0:3262            0.0.0.0:*               LISTEN      14836/iscsi_snapsho
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      14850/nginx: master
tcp        0      0 0.0.0.0:5001            0.0.0.0:*               LISTEN      14850/nginx: master
udp        0      0 0.0.0.0:1900            0.0.0.0:*                           13399/minissdpd
udp        0      0 0.0.0.0:34769           0.0.0.0:*                           16698/avahi-daemon:
udp        0      0 0.0.0.0:48899           0.0.0.0:*                           12766/synosnmpcd
udp     1280      0 0.0.0.0:68              0.0.0.0:*                           10888/dhclient
udp        0      0 192.168.200.144:123     0.0.0.0:*                           13070/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           13070/ntpd
udp        0      0 0.0.0.0:123             0.0.0.0:*                           13070/ntpd
udp        0      0 192.168.200.255:137     0.0.0.0:*                           16619/nmbd
udp        0      0 192.168.200.144:137     0.0.0.0:*                           16619/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                           16619/nmbd
udp        0      0 192.168.200.255:138     0.0.0.0:*                           16619/nmbd
udp        0      0 192.168.200.144:138     0.0.0.0:*                           16619/nmbd
udp        0      0 0.0.0.0:138             0.0.0.0:*                           16619/nmbd
udp        0      0 127.0.0.1:161           0.0.0.0:*                           12436/snmpd
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           16698/avahi-daemon:
udp        0      0 0.0.0.0:9997            0.0.0.0:*                           13027/findhostd
udp        0      0 0.0.0.0:9998            0.0.0.0:*                           13027/findhostd
udp        0      0 0.0.0.0:9999            0.0.0.0:*                           13027/findhostd
```

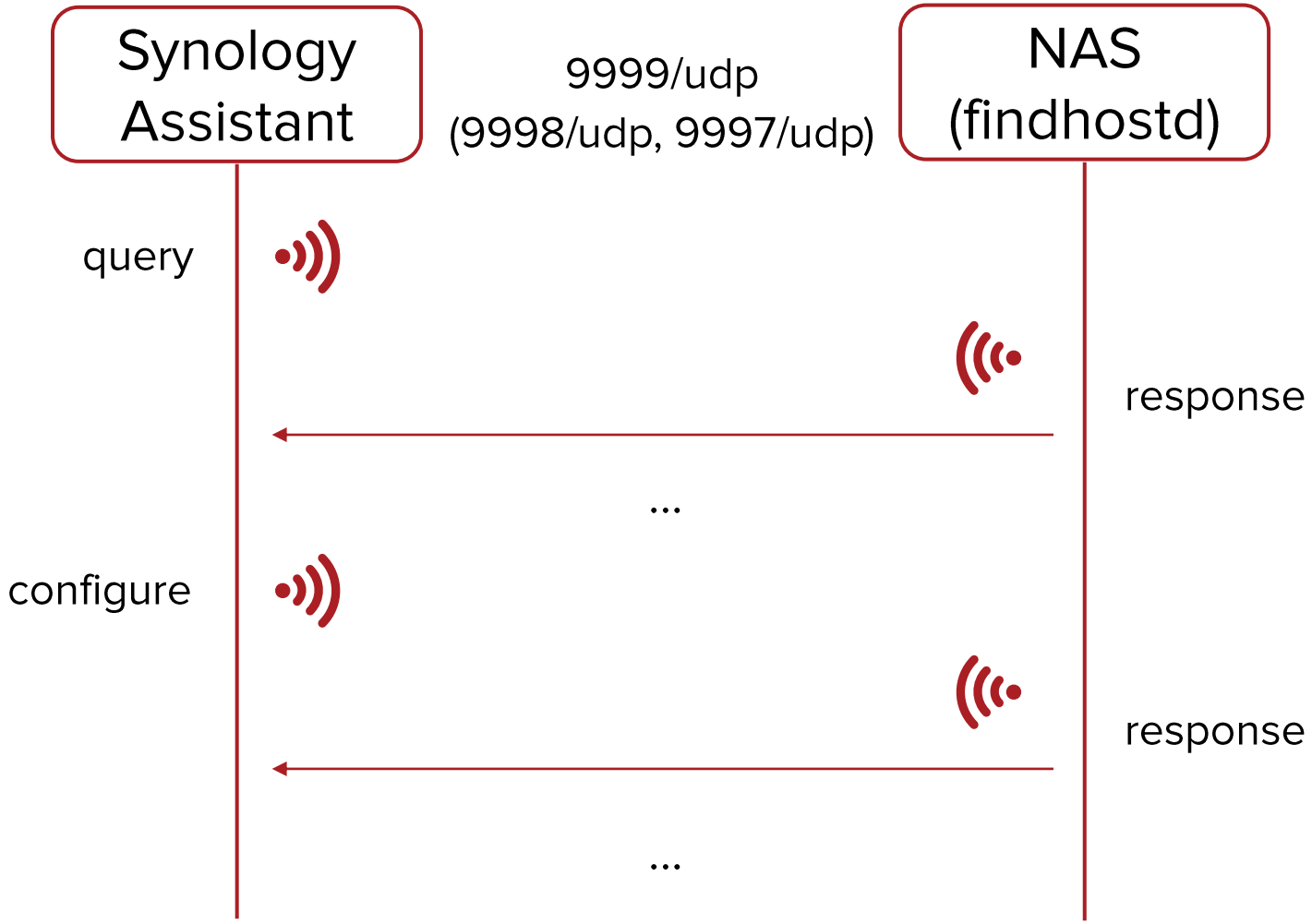
Services: findhostd

- findhostd is responsible for communicating with the Synology Assistant
- Synology Assistant is a desktop utility that searches for DiskStation in LAN
  - 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?

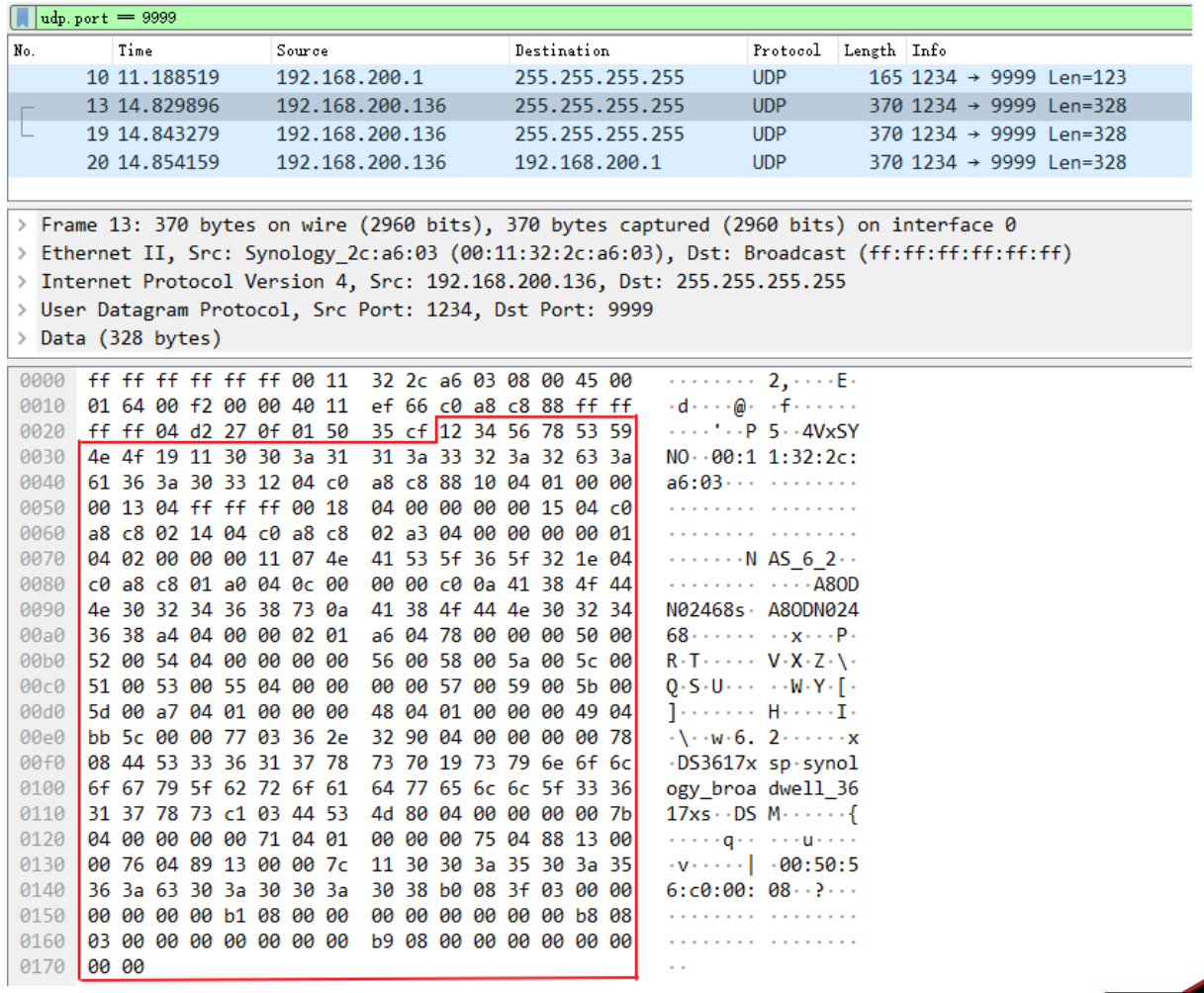


Services: findhostd



Services: findhostd

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

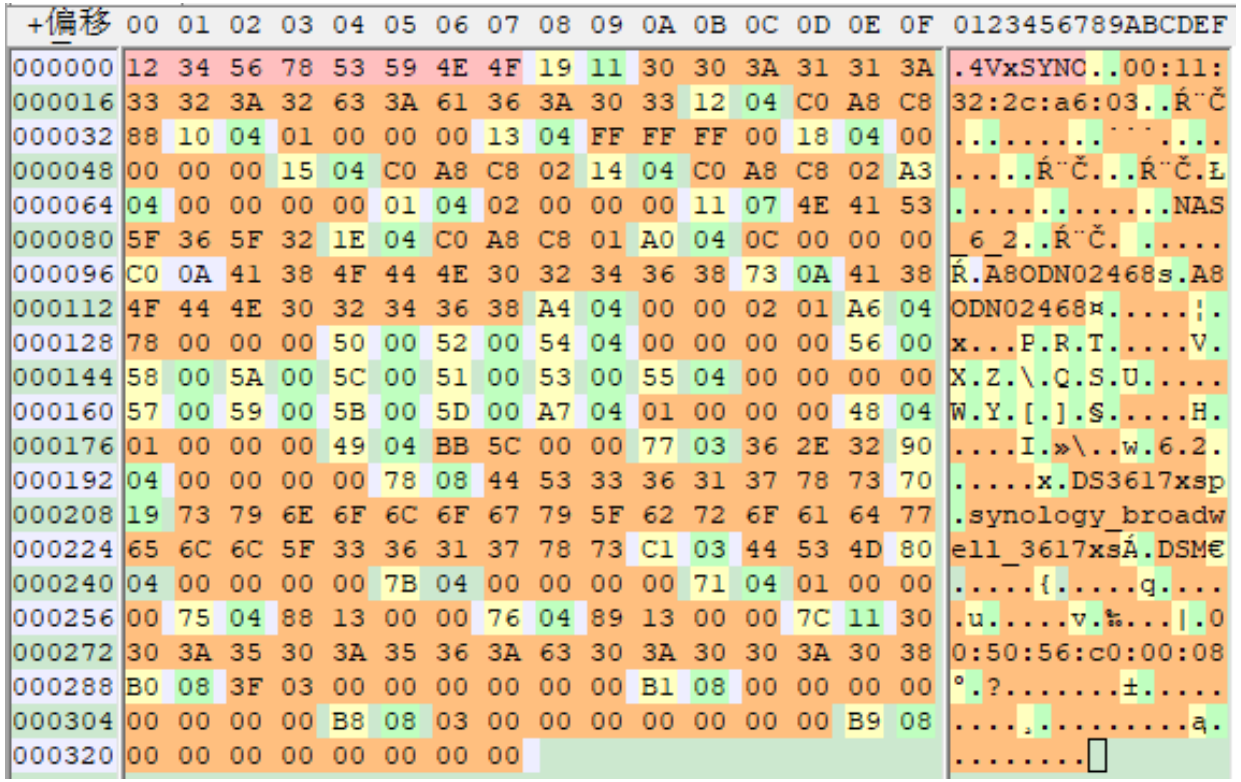


Services: findhostd

```
#define magic_plain “\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
00000010 00000001 00000e8c 00000004 00000000 00000000
00000011 00000000 00000008 00000024 00000000 00000000   # hostname
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
...
00000020 00000001 00000e8c 00000004 00000000 00000004   # packet subtype
...
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   # buildnumber
0000004a 00000000 00000c24 000001f0 00000000 00000000   # username
0000004b 00000003 00000000 00000000 00000000 00000000   # shared folder name
...
00000070 00000000 00000bb0 00000044 00000000 00000000   # unique
00000071 00000001 00000ec4 00000004 00000000 00000000   # supportraid
...
00000075 00000001 00000eac 00000004 00000000 00000000   # port
00000076 00000001 00000eb0 00000004 00000000 00000000   # ssl port
00000077 00000000 00000e14 00000008 00000000 00000000   # productversion
00000078 00000000 00000e24 00000030 00000000 00000000   # upnpmodelname
00000079 00000001 00000ee0 00000004 00000000 00000000   # memtester error code
...
000000a7 00000001 00000eb4 00000004 00000000 00000000   # bootsep num
...
000000c0 00000000 00002f1c 00000020 00000000 00000000   # serial number
000000c1 00000000 00002f40 00000008 00000000 00000000   # os_name
000000c2 00000001 00002f48 00000004 00000000 00000000
```

Services: findhostd

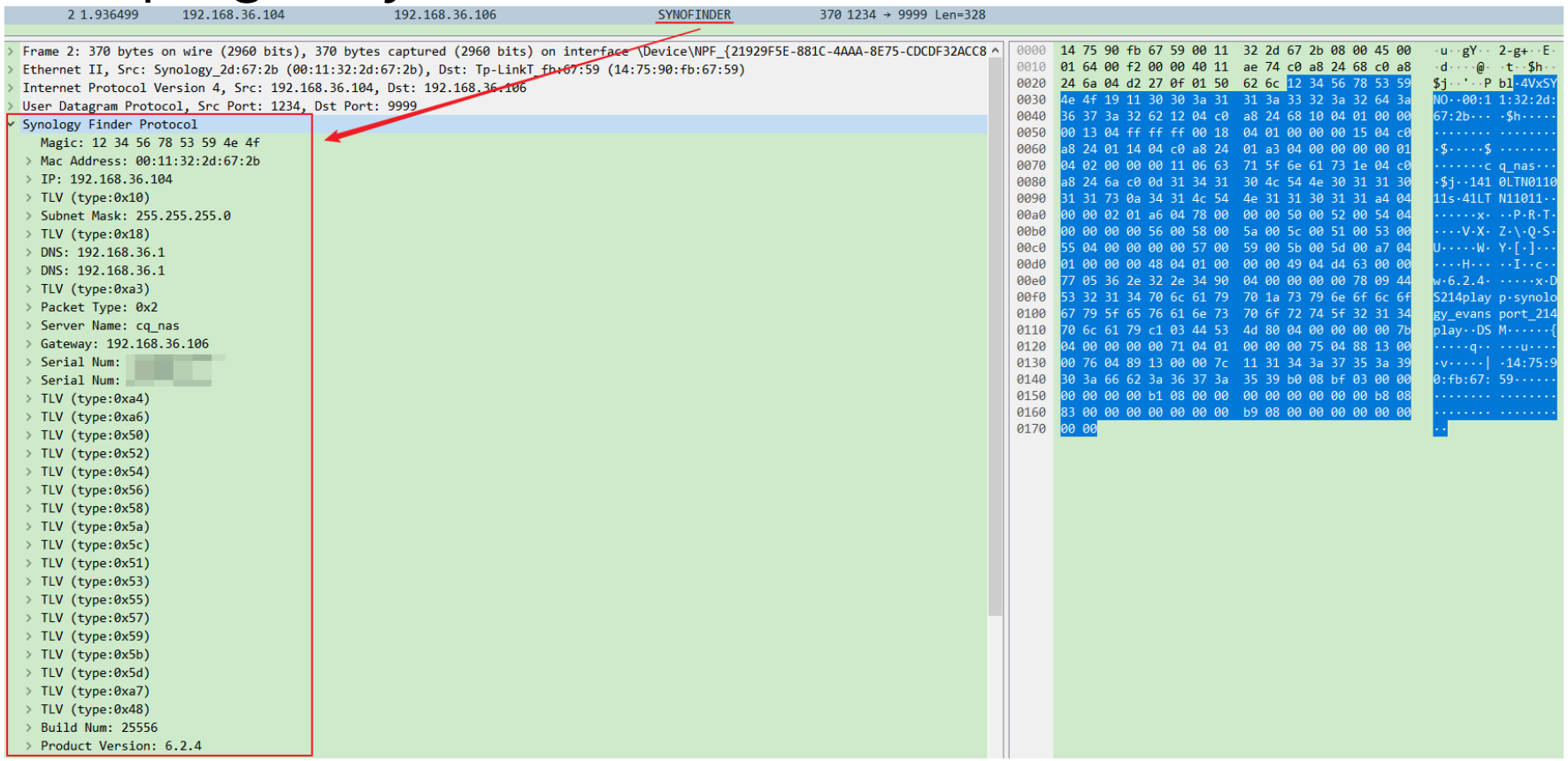


+偏移	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
000000	12	34	56	78	53	59	4E	4F	19	11	30	30	3A	31	31	3A	.4VxSYNO..00:11:
000016	33	32	3A	32	63	3A	61	36	3A	30	33	12	04	C0	A8	C8	32:2c:a6:03..Ŕ¨Č
000032	88	10	04	01	00	00	00	13	04	FF	FF	FF	00	18	04	00	ˆ.....¨.....˙˙˙....
000048	00	00	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	71	04	01	00	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	....¸.........ą.
000320	00	00	00	00	00	00	00	00									....

- Message format
  - magic
  - pkt_id
  - data_length
  - data

Services: findhostd

- Wireshark plugin: syno_finder

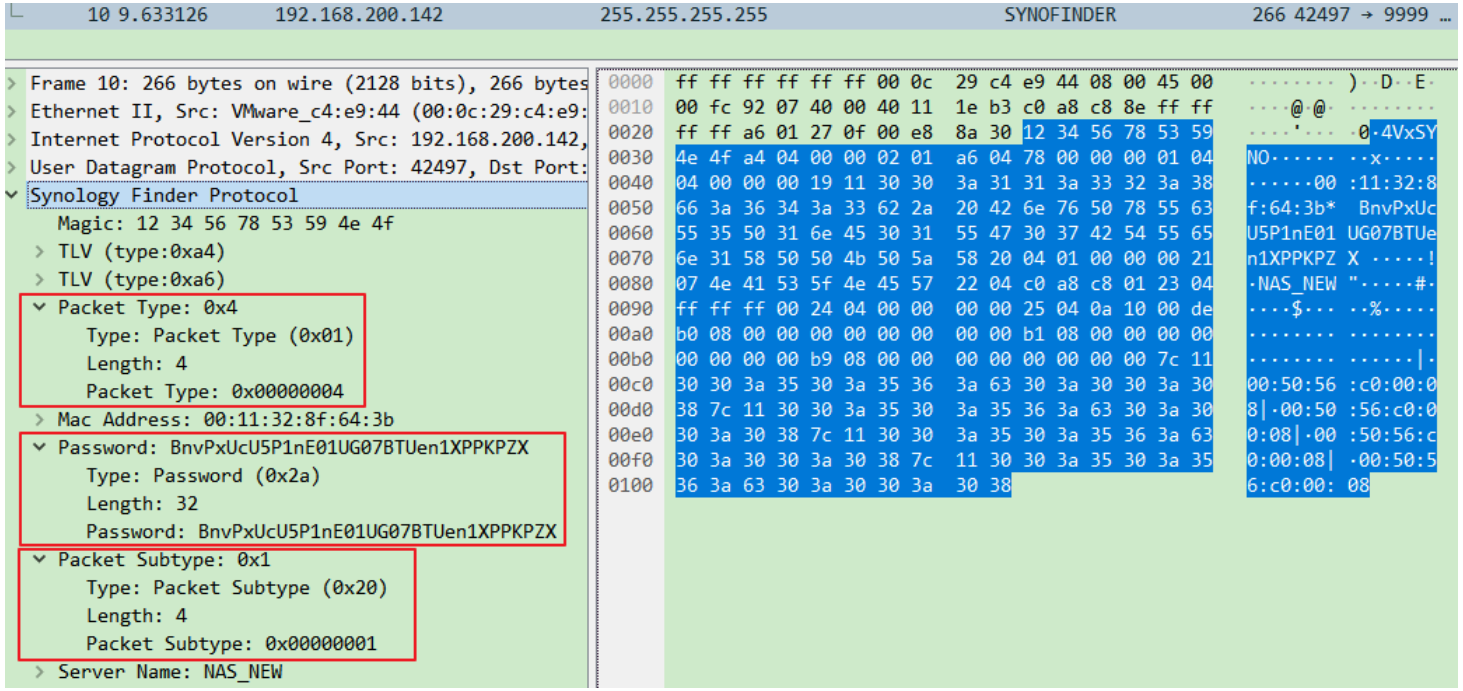


- Available: https://github.com/cq674350529/pocs_slides/scripts/wireshark_plugins/syno_finder

Services: findhostd

#1 password leakage

- Common packet types
  - 0x1: broadcast query
  - 0x3: netsetting
  - 0x4: quickconf
  - 0x5: share access query
  - 0x7: redirector share query
  - 0x9: DR2 auth query
  - 0xc: memory test
  - 0xd: share enum
- netsetting/quickconf/memtest packet
  - pkt_id=0x2a: encoded password



Plaintext password can be obtained by calling MatrixDecode().

In some cases, an adversary can easily steal the plaintext administrator password by monitoring the broadcast traffic.

Services: findhostd

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

With Scapy, we can define the protocol format easily and quickly.

```
class IDPacket(Packet):
    fields_desc = [
        XByteField('id', 0x01),
        FieldLenField('length', None, length_of='value', fmt='B', adjust=lambda pkt,x:x),
        StrLenField('value', '\x01\x00\x00\x00', length_from=lambda x:x.length)
    ]

    def post_build(self, pkt, pay):
        if pkt[1] != 4 and pkt[1] != 0xff:
            packet_max_len = self._get_item_max_len(pkt[0])
            if len(pkt[2:]) >= packet_max_len:
                if packet_max_len == 0:
                    pkt = bytes([pkt[0], 0])
                else:
                    pkt = bytes([pkt[0], packet_max_len-1])+ pkt[2:2+packet_max_len]
        return pkt + pay

class FindHostPacket(Packet):
    fields_desc = [
        StrLenField('maigc_plain', '\x12\x34\x56\x78\x53\x59\x4e\x4f'),
        PacketListField('id_packets', [], IDPacket)
    ]
```

Services: findhostd

- Protocol fuzzing: Kitty & Scapy

```
packet_id_a4 = qh_nas_protocols.IDPacket(id=0xa4, value='\x00\x00\x02\x01')
# ...
packet_id_2a = qh_nas_protocols.IDPacket(id=0x2a, value=RandBin(size=240))
# ...
pakcet_id_rand1 = qh_nas_protocols.IDPacket(id=RandByte(), value=RandBin(size=0xff))
pakcet_id_rand2 = qh_nas_protocols.IDPacket(id=RandChoice(*qh_nas_protocols.PACKET_IDS), value=RandBin(size=0xff))
findhost_packet = qh_nas_protocols.FindHostPacket(id_packets=[packet_id_a4, packet_id_2a, ..., pakcet_id_rand1, pakcet_id_rand2])

findhost_template = Template(name='template_1', fields=[ScapyField(findhost_packet, name='scapy_1', seed=RANDSEED, fuzz_count=100000)])
model = GraphModel()
model.connect(findhost_template)

target = UdpTarget(name='qh_nas', host=host, port=port, timeout=2)

fuzzer = ServerFuzzer()
fuzzer.set_interface(WebInterface(host='0.0.0.0', port=26001))
fuzzer.set_model(model)
fuzzer.set_target(target)
fuzzer.start()
```

- With Kitty, we can reuse the pre-defined protocol format to set up a black-box fuzzer easily and quickly.
- We can fuzz both the findhostd and Synology Assistant at the same time ☺

Services: findhostd

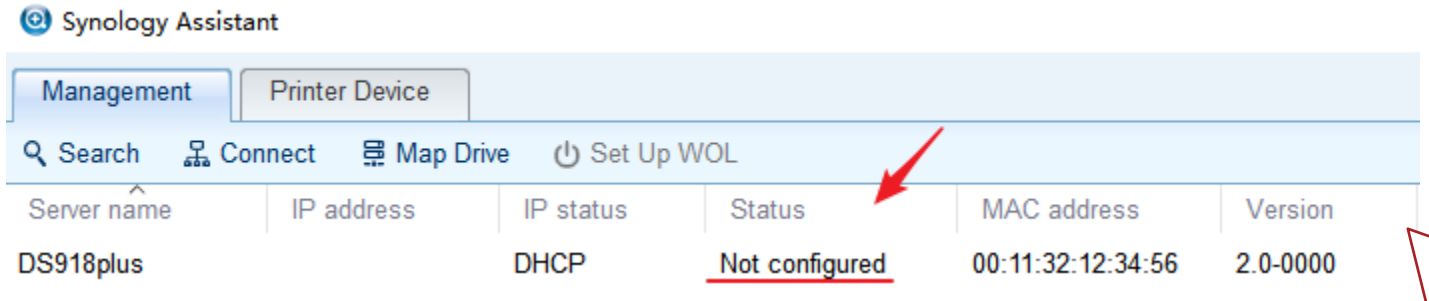
- Protocol fuzzing: Kitty & Scapy

With the pre-defined protocol format, we can also build a simple Synology Assistant client with python.

```python
class DSAssistantClient:
    # ...

    def add_pkt_field(self, pkt_id, value):
        self.pkt_fields.append(qh_nas_protocols.IDPacket(id=pkt_id, value=value))

    def find_target_nas(self):
        self.clear_pkt_fields()

        self.add_pkt_field(0xa4, '\x00\x00\x02\x01')
        self.add_pkt_field(0xa6, '\x78\x00\x00\x00')
        self.add_pkt_field(0x01, p32(0x1))  # packet type
        # ...
        self.add_pkt_field(0xb9, '\x00\x00\x00\x00\x00\x00\x00\x00')
        self.add_pkt_field(0x7c, '00:50:56:c0:00:08')

        self.build_send_packet()

    def quick_conf(self):
        self.clear_pkt_fields()

        self.add_pkt_field(0xa4, '\x00\x00\x02\x01')
        self.add_pkt_field(0xa6, '\x78\x00\x00\x00')
        self.add_pkt_field(0x01, p32(0x4))  # packet type
        self.add_pkt_field(0x20, p32(0x1))  # packet subtype
        self.add_pkt_field(0x19, '00:11:32:8f:64:3b')
        self.add_pkt_field(0x2a, 'BnvPxUcU5P1nE01UG07BTUen1XPPKPZX')
        self.add_pkt_field(0x21, 'NAS_NEW')
        self.add_pkt_field(0x22, '\xc0\xa8\xc8\x01')
        # ...
        self.add_pkt_field(0xb9, "\x00\x00\x00\x00\x00\x00\x00\x00")
        # ...
        self.add_pkt_field(0x7c, "00:50:56:c0:00:08")

        self.build_send_packet()

    # ...

if __name__ == "__main__":
    ds_assistant = DSAssistantClient("ds_assistant")
    ds_assistant.find_target_nas()
    # ...
```

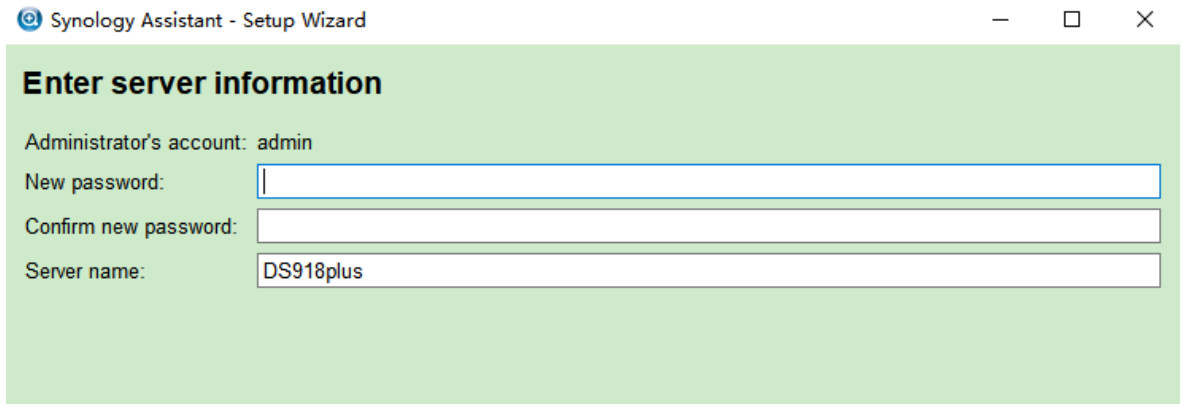
Services: findhostd

#2 password stealing



During fuzzing, the configured DS918plus becomes "Not configured".

Did some crafted packets reset the DS918plus?
☹ It only deceived the Synology Assistant.



Password leakage again when re-configuring the device

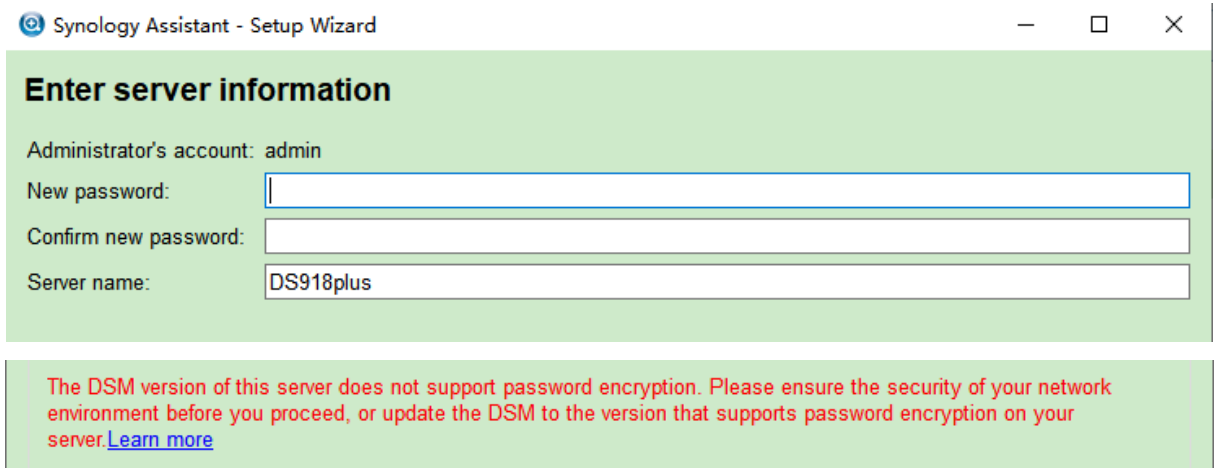
An adversary can cheat the administrator into re-configuring the device, then steal the plaintext administrator password by monitoring the broadcast traffic.

Services: findhostd

- Changes

```
#define magic_plain “\x12\x34\x56\x78\x53\x59\x4e\x4f”
#define magic_encrypted “\x12\x34\x55\x66\x53\x59\x4e\x4f” // introduced recently
```

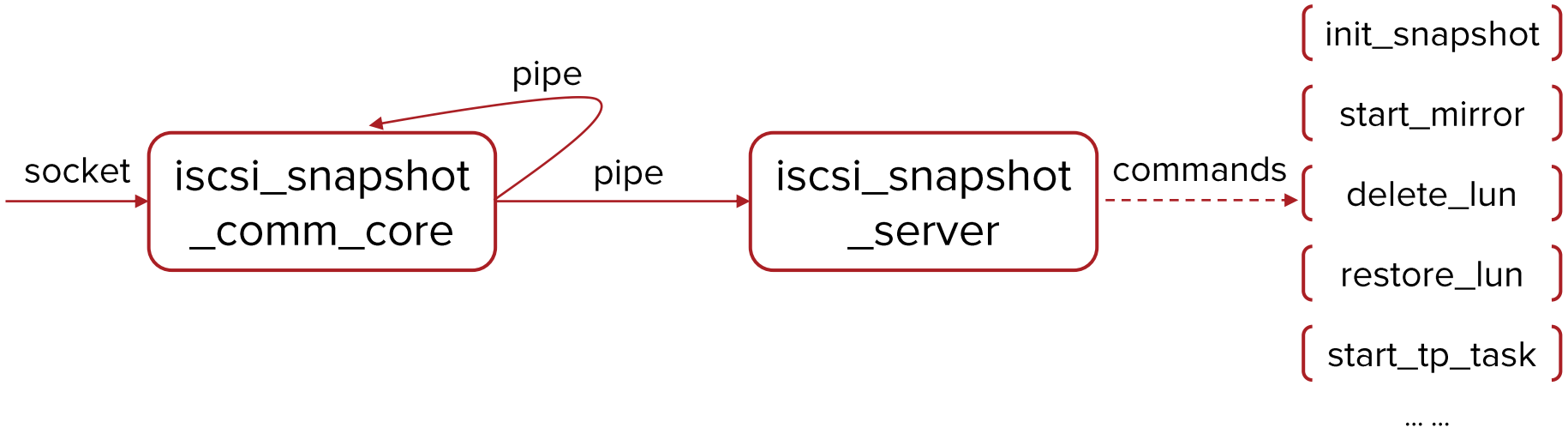
```
000000c3 00000001 00002f48 00000004 00000000 00000000   # support_onsite_tool   <== new added
000000c4 00000000 00002f4c 00000041 00000000 00000000   # public key
000000c5 00000001 00002f90 00000004 00000000 00000000   # randombytes
000000c6 00000001 00002f94 00000004 00000000 00000000
```



- The messages are encrypted if using a more recent Synology Assistant or DSM.
- Password stealing is still possible ☺

Services: 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



Services: iscsi_snapshot_comm_core #3 signed comparison


```
__int64 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);
  // ...
  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 comparison
    v4 = *(_DWORD *)v7;
  memcpy(dest, v7[1], (signed int)v4);   // overflow
    // ...
```

```
ssize_t 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;
}
```

Services: 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            0xffffffffffffdf8df       -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
```

Services: iscsi_snapshot_comm_core


```
signed __int64 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 *, __int64))(*(_QWORD *)(v4 + 56) + 112LL))(v4, v5, 4096LL); // recv msg
    // ...
    v7 = v5[1];
    if ( v5[1] == 1 || *v5 == 16 || *v5 == -1 )
    {
      switch ( *v5 + 1 )
      {
        case 0:
          HandleRejectMsg(v5);  continue;
        // ...
        case 33:
          HandleSendMsg(v5);  continue;
        case 34:
          HandleRecvMsg(v5);  continue;
        case 49:
          HandleBindMsg(v5);    continue;
        // ...
```

```
__int64 HandleRecvMsg(__int64 a1)
{
  v1 = SearchAppInLocalHostSetByUUID(a1 + 36);
  v2 = (void *)v1;
  if ( v1 )
  {
    v3 = -((int)AppSendControl(v2, a1, (unsigned int)(*(_DWORD *)(a1 + 76) + 84)) <= 0);
  }
  // ...
}
```

external controllable

Services: iscsi_snapshot_comm_core #4 out-of-bounds read


```
__int64 PacketWrite(__int64 a1, __int64 (__fastcall *a2)(__int64, void *, _QWORD), __int64 a3, unsigned int 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 CreatePacket(__int64 *a1, const void *a2, int a3)
{
  if ( a1
    && (v3 = a3 + 32,
        v4 = a3,
        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);  // out-of-bounds read
  }
  // ...
}
```

- a small large value(e.g. 0x1100): out-of-bounds read
- a big large value(e.g. 0xffffff90): integer overflow

Services: iscsi_snapshot_comm_core #4 out-of-bounds read

These two functions have an undefined length.

```
dq offset aGetappip      ; "GetAppIP"
dq 44h
dq 19h
dq offset aGetappipack   ; "GetAppIPAck"
dq 0Ch  <-- length
dq 20h
dq offset aSendmsg       ; "SendMsg"
dq 0    <--
dq 21h
dq offset aRecvmsg       ; "RecvMsg"
dq 0    <-- undefined
dq 30h
dq offset aFailToBind+8 ; "Bind"
dq 0D4h
dq 31h
dq offset aUbond+1       ; "Bond"
```

```
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            0xfffffffe0      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
```

Services: iscsi_snapshot_comm_core


```
signed __int64 sub_401BA0()
{
  // ...
  v0 = (_QWORD *)CreateSynoCommEvlp();
  v1 = CreateSynoComm("ISS-SERVER");
  // ...
  while ( 1 )
  {
    while ( 1 )
    {
      v2 = CommRecvEvlp(v1, v0);    // recv data
      // ...
      ExtractFromUUIDByDataPacket(*v0, v64);
      ExtractToUUIDByDataPacket(*v0, v65);
      v4 = (const char *)CommGetEvlpData(v0);
      // ...
      v5 = CommGetEvlpData(v0);
      v6 = HandleProtCommand(v1, v5, &s, v64);
      // ...
```

```
__int64 HandleProtCommand(__int64 a1, __int64 a2, const char **a3, __int64 a4)
{
  // ...
  v5 = GetJSONFromString(a2);
  // ...
  v9 = (const char *)SYNOCPBJsonGetString(v5, "command", 0LL);
  // ...
  v10 = 0;
  v11 = (const char *)*((_QWORD *)pCmdPatterns_ptr + 1);
  v12 = (char *)pCmdPatterns_ptr + 32;
  // ...
  v25 = (unsigned int *)((char *)pCmdPatterns_ptr + 24 * v10);
  v26 = *v25;
  if ( !(unsigned int)json_object_object_get_ex(v6, "command", &v33) ) v33 = 0LL;
  if ( !(unsigned int)json_object_object_get_ex(v6, "command_sn", &v34) ) v34 = 0LL;
  if ( !(unsigned int)json_object_object_get_ex(v6, "plugin_id", &v35) ) v35 = 0LL;
  if ( !(unsigned int)json_object_object_get_ex(v6, "key", &v36) ) v36 = 0LL;
  if ( !(unsigned int)json_object_object_get_ex(v6, "protocol_version", &v37) ) v37 = 0LL;
  // ...
  v38 = json_object_get_string(v33, "protocol_version");
  // ...
  if ( v42 && *v42 == 50 )
  {
    v29 = (*((__int64 (__fastcall **)(__int64, const char *, __int64 *, const void **,
__int64))pCmdPatterns_ptr + 3 * v24 + 2))( a1, v6, &v38, &v32, a4);
    // ...
```

Services: iscsi_snapshot_comm_core #5 improper access control


```
dq 1                    ; DATA XREF: LOAD:pCmdPatterns_ptr↑o
dq offset aUnregister_0+2 ; "register"
dq offset HandleProtRegister
dq 2
dq offset aDisconnect+3 ; "connect"
dq offset HandleProtConnect
dq 3
dq offset aDisconnect   ; "disconnect"
dq offset HandleProtDisConnect
dq 4
dq offset aUnregister_0 ; "unregister"
dq offset HandleProtUnRegister
dq 5
dq offset aInitSnapshot ; "init_snapshot"
dq offset HandleProtInitSnapshot
dq 6
dq offset aIsLunSupported ; "is_lun_supported"
dq offset HandleProtIsLunSupport
dq 7
dq offset aStartMirror  ; "start_mirror"
dq offset HandleProtStartMirror
dq 8
dq offset aIsMirrorDone ; "is_mirror_done"
dq offset HandleProtIsMirrorDone
dq 9
dq offset aDepartRelation ; "depart_relation"
dq offset HandleProtDepartRelation
dq 0Ah
dq offset aAbortTask    ; "abort_task"
dq offset HandleProtAbortTask
dq 0Bh
dq offset aGetMirroredLun ; "get_mirrored_lun"
dq offset HandleProtGetMirroredLun
dq 0Ch
dq offset aCreateMappedTa ; "create_mapped_target"
dq offset HandleProtCreateMappedTarget
dq 0Dh
dq offset aBadDeleteLun+4 ; "delete_lun"
dq offset HandleProtDeleteLun
dq 0Eh
dq offset aRestoreLun   ; "restore_lun"
dq offset HandleProtRestoreLun
dq 0Fh
```

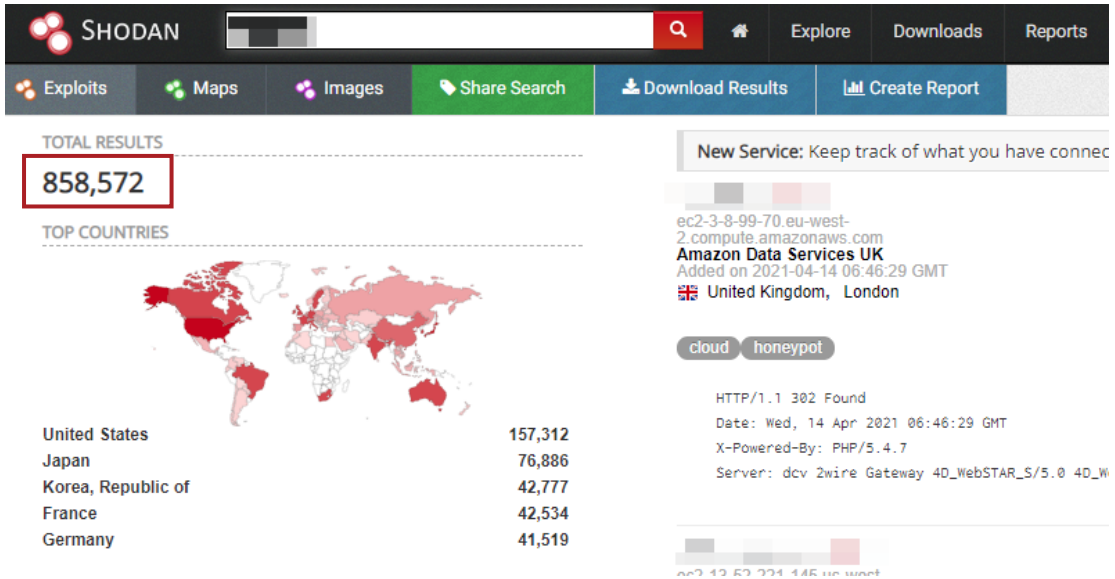
```
signed __int64 HandleProtDeleteLun(__int64 a1, __int64 a2, __int64 a3, _QWORD *
a4)
{
  v16[0] = 0LL;
  if ( !(unsigned int)json_object_object_get_ex(a2, "data", v16) )
  {
    // ...
  }
  v7 = SYNOCPBJsonGetInteger(v16[0], "type");
  v8 = v7;
  // ...
  v9 = SYNOCPBJsonGetString(v16[0], "lun", 0LL);
  // ...
  v10 = v9;
  v11 = SYNOCPBGetLun(v8, v9);
  v12 = (unsigned int *)v11;
  // ...
  if ( (unsigned int)SYNOiSCSILunDelete(v11, v10) )
  {
    //
```

No authentication is required.

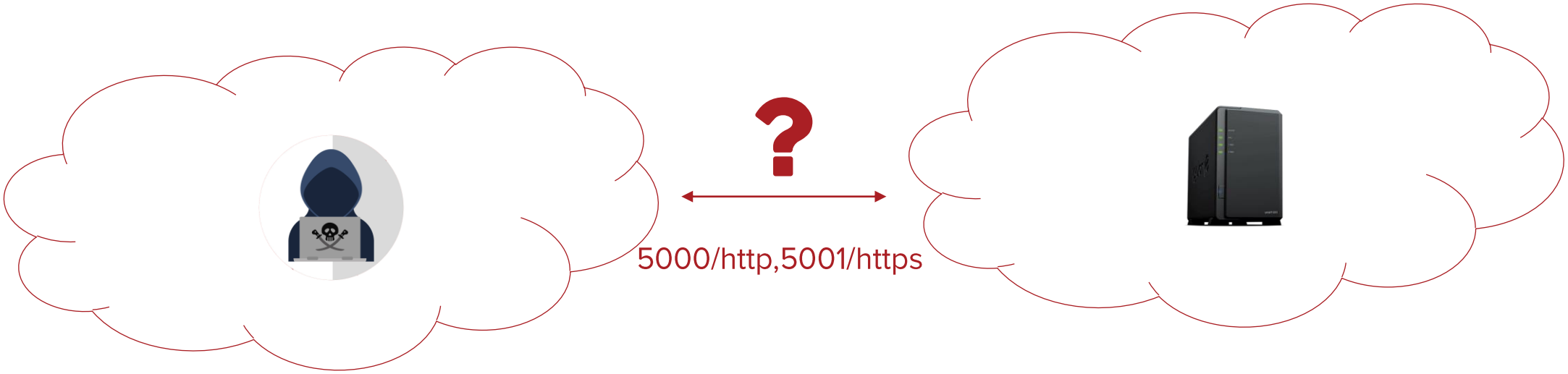
It's possible for an unauthenticated adversary to delete luns on the device, which may pose threat to data.

Remote Adversary's Perspective

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



Remote Adversary's Perspective



wide area network

Device Fingerprinting

- Port: 5000/5001 (default)
- Shodan query: html:"SYNO.Core.Desktop.SessionData"

```
<style type="text/css">
@import url("webman/modules/LogCenter/style.css?v=1589235133");
<!-- ... -->
@import url("webman/modules/ExternalDevices/style.css?v=1589235155");
</style>
<style type="text/css">
@import url("webman/modules/HelpBrowser/style.css?v=1589235155");
<!-- ... -->
@import url("webman/modules/PersonalSettings/style.css?v=1589235155");
</style>
<link rel="stylesheet" type="text/css" href="webman/3rdparty/Virtualization/style.css?v=1610705236" />
<link rel="stylesheet" type="text/css" href="webman/3rdparty/AudioStation/style.css?v=1611057399" />
</head>
<script type="text/javascript" src="webapi/entry.cgi?api=SYNO.Core.Desktop.Defs&version=1&method=getjs&v=1609215848"></script>
<!-- ... -->
<script type="text/javascript" src="webapi/entry.cgi?api=SYNO.Core.Desktop.SessionData&version=1&method=getjs&SynoToken=&v=1589235146"></script>
```

inbuilt modules

installed packages

AudioStation version: 6.5.6-3377 ☺

Index of / download / Os / DSM / 6.2.3-25426

Name	Last modified
Parent Directory	
DSM_DDSM_25426.pat	Thu, 14 May 2020 01:51:00 GMT
DSM_DS1019+_25426.pat	Tue, 12 May 2020 02:14:50 GMT
DSM_DS111_25426.pat	Tue, 12 May 2020 02:15:02 GMT
DSM_DS112+_25426.pat	Tue, 12 May 2020 02:15:25 GMT
DSM_DS112_25426.pat	Tue, 12 May 2020 02:15:14 GMT
DSM_DS112j_25426.pat	Tue, 12 May 2020 02:15:36 GMT

v=1589235146: modify_timestamp

==> 2020-05-12 06:12:26

DSM version: 6.2.3-25426 ☺

Http Request Process Flow

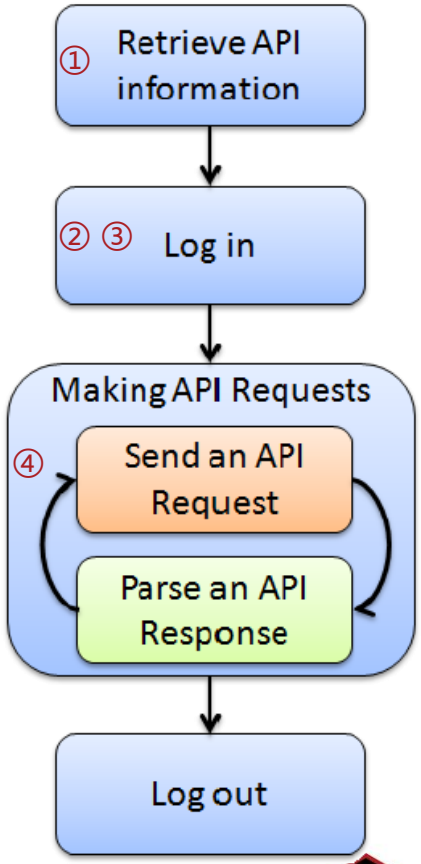
- 5000/http (or 5001/https) is the main entry for all HTTP requests

#	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:
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;
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: 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","normal.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)

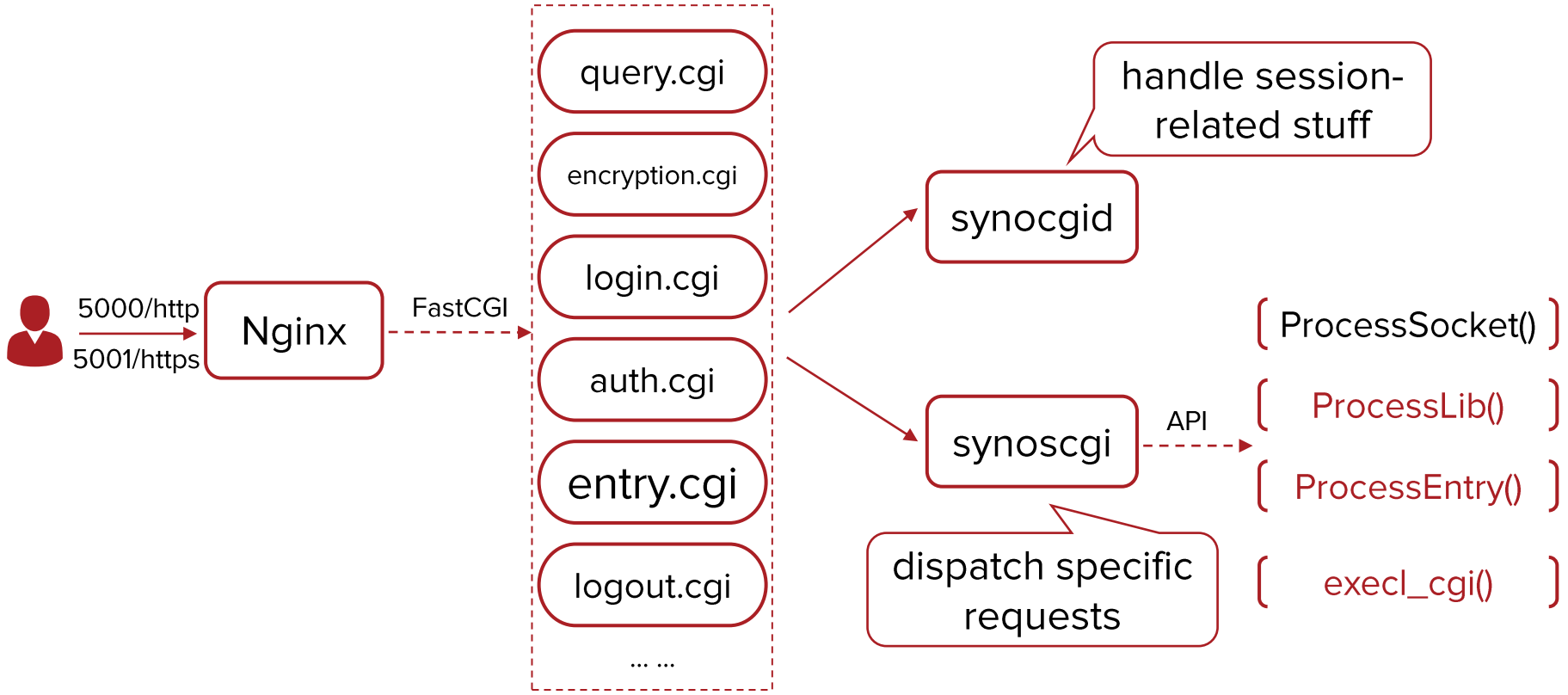
the file to handle this request

which methods are available and the corresponding version

overwrite the definition above

Http Request Process Flow

- A simple and high-level process flow

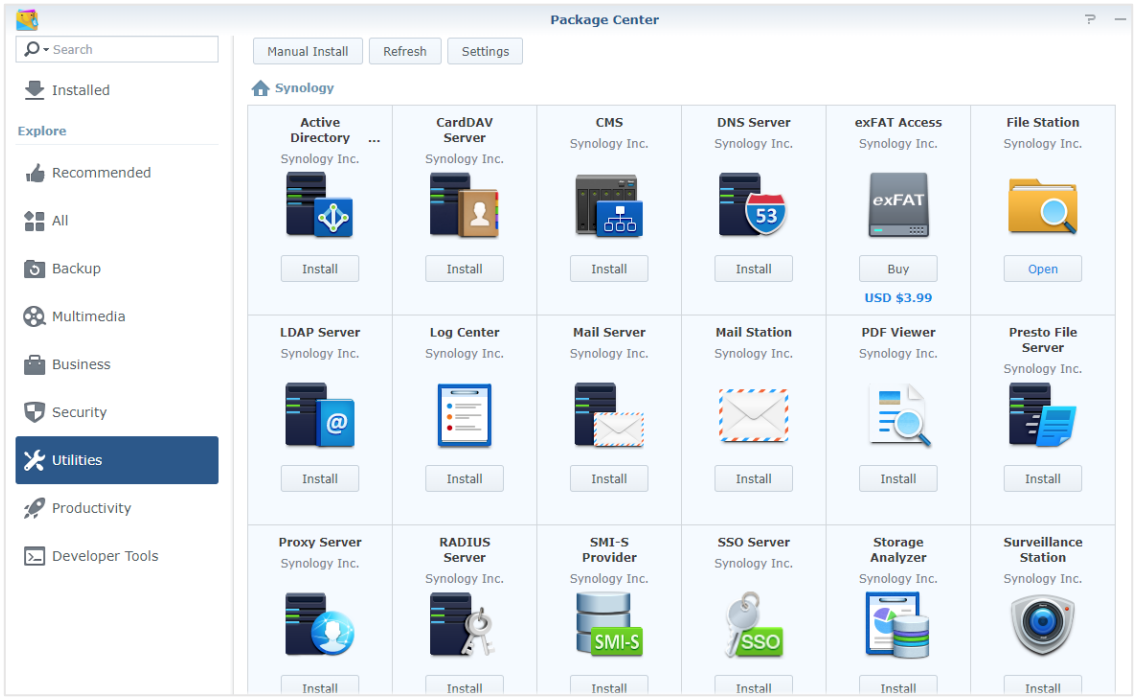


Remote Attack Surface

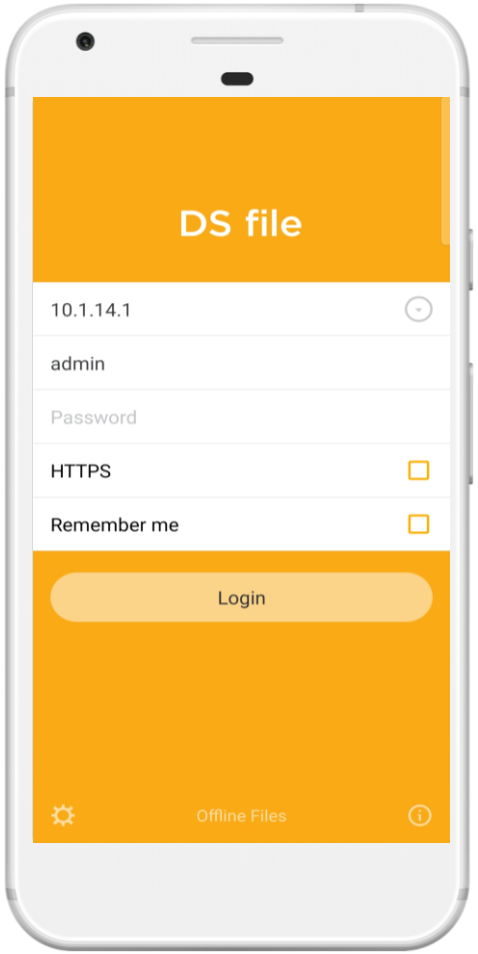
- DSM (DiskStation Manager)

```
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.VPNPassthrough.so        webapi_gpo_client.so
```

- Packages



DS file App



- Securely browse folders and files on your DiskStation with your Android device
- Transfer files between the device and the DiskStation
- Manage your files while you are away whenever an Internet connection is available

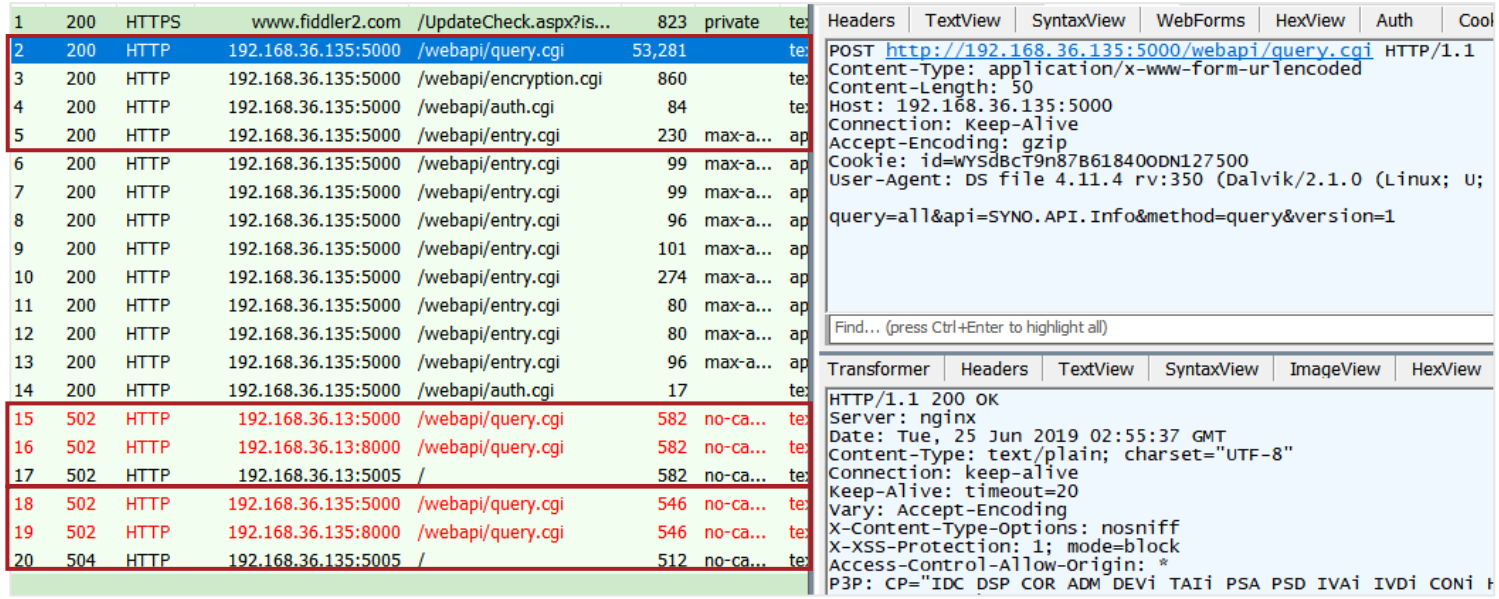
DS file App

- When try to login into the DiskStation

In normal case, use PKI based encryption for authentication

input a wrong server ip (or server name)

network is not temporarily available



#	Result	Protocol	Host	URL	Body	Caching	Content-Type
1	200	HTTPS	www.fiddler2.com	/UpdateCheck.aspx?is...	823	private	te
2	200	HTTP	192.168.36.135:5000	/webapi/query.cgi	53,281		te
3	200	HTTP	192.168.36.135:5000	/webapi/encryption.cgi	860		te
4	200	HTTP	192.168.36.135:5000	/webapi/auth.cgi	84		te
5	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	230	max-a...	ap
6	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	99	max-a...	ap
7	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	99	max-a...	ap
8	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	96	max-a...	ap
9	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	101	max-a...	ap
10	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	274	max-a...	ap
11	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	80	max-a...	ap
12	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	80	max-a...	ap
13	200	HTTP	192.168.36.135:5000	/webapi/entry.cgi	96	max-a...	ap
14	200	HTTP	192.168.36.135:5000	/webapi/auth.cgi	17		te
15	502	HTTP	192.168.36.13:5000	/webapi/query.cgi	582	no-ca...	te
16	502	HTTP	192.168.36.13:8000	/webapi/query.cgi	582	no-ca...	te
17	502	HTTP	192.168.36.13:5005	/	582	no-ca...	te
18	502	HTTP	192.168.36.135:5000	/webapi/query.cgi	546	no-ca...	te
19	502	HTTP	192.168.36.135:8000	/webapi/query.cgi	546	no-ca...	te
20	504	HTTP	192.168.36.135:5005	/	512	no-ca...	te

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cool

```
POST http://192.168.36.135:5000/webapi/query.cgi HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Host: 192.168.36.135:5000
Connection: Keep-Alive
Accept-Encoding: gzip
Cookie: id=WYSdBcT9n87B6184ODN127500
User-Agent: DS file 4.11.4 rv:350 (Dalvik/2.1.0 (Linux; U;

query=all&api=SYNO.API.Info&method=query&version=1
```

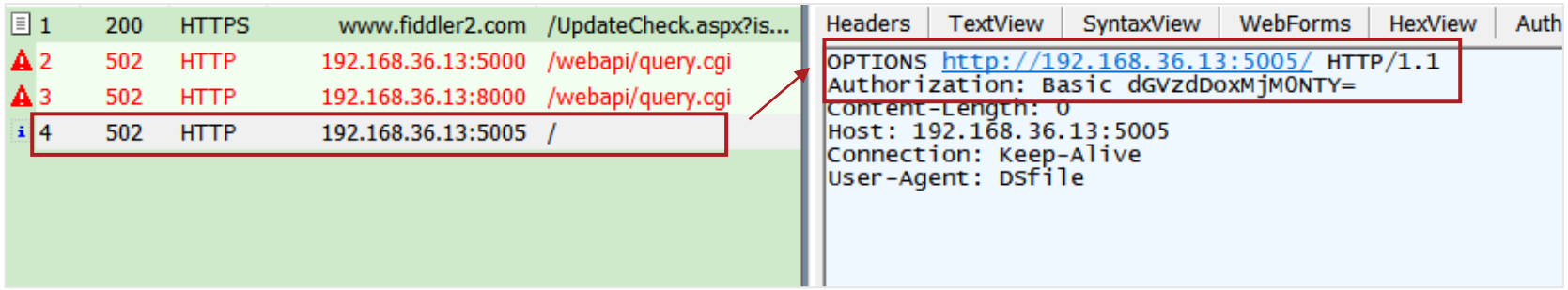
Find... (press Ctrl+Enter to highlight all)

Transformer | Headers | TextView | SyntaxView | ImageView | HexView

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 25 Jun 2019 02:55:37 GMT
Content-Type: text/plain; charset="UTF-8"
Connection: keep-alive
Keep-Alive: timeout=20
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: *
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi H
```

DS file App

#6 password leakage

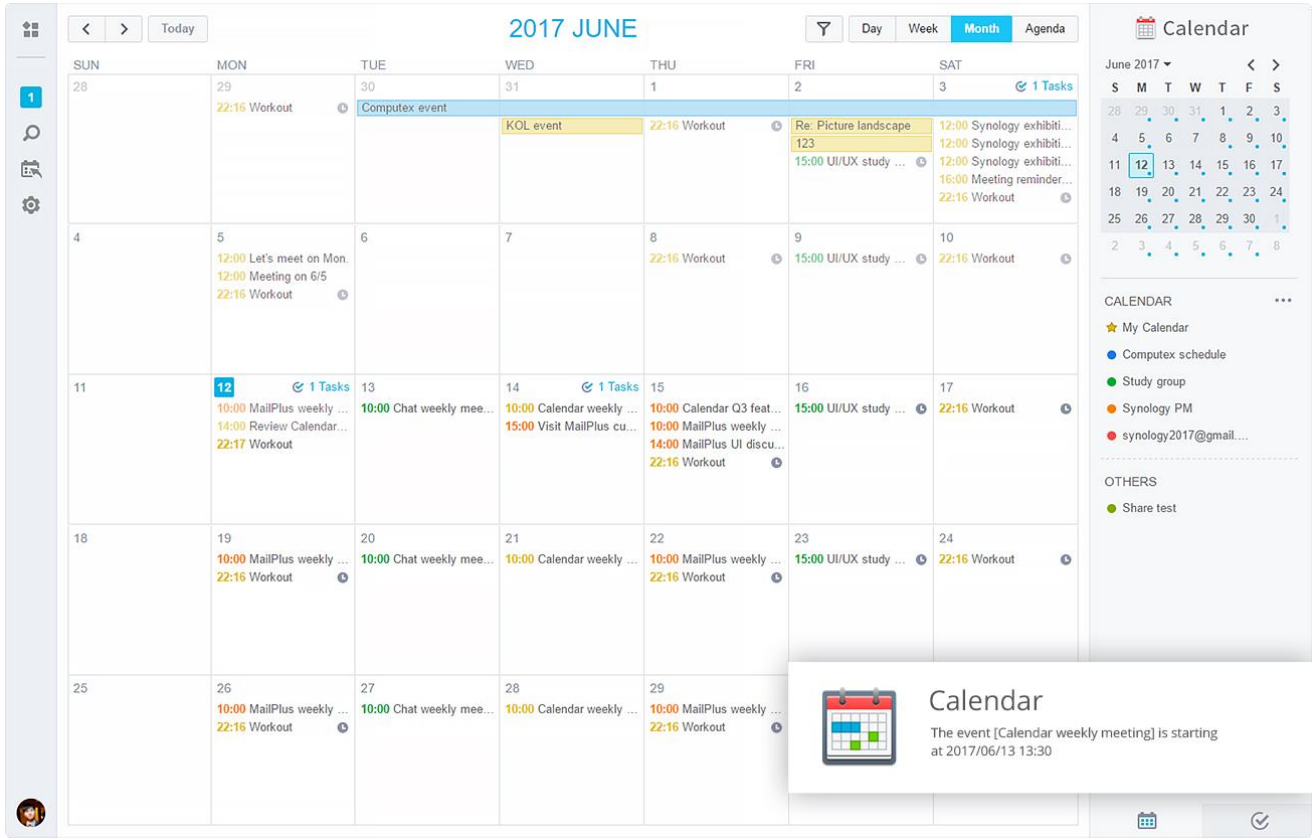


test:12
3456

In unsafe network environments, by simply dropping or redirecting specific requests, a MitM adversary can obtain the plaintext password. It applies even if https mode is used.

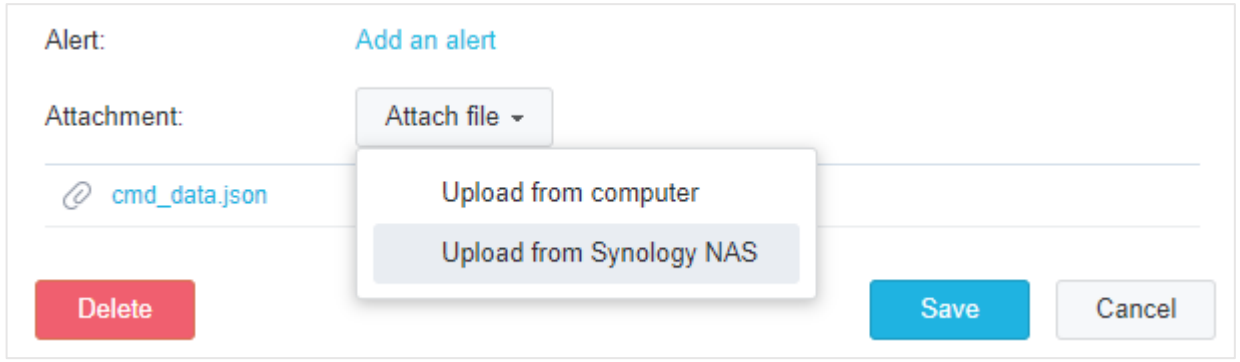
Synology Calendar

- A web-based application for organizing and planning out daily events
- Create events in your own personal calendar or share a calendar within a group of people
- Support adding attachments to events



Synology Calendar

#7 directory traversal

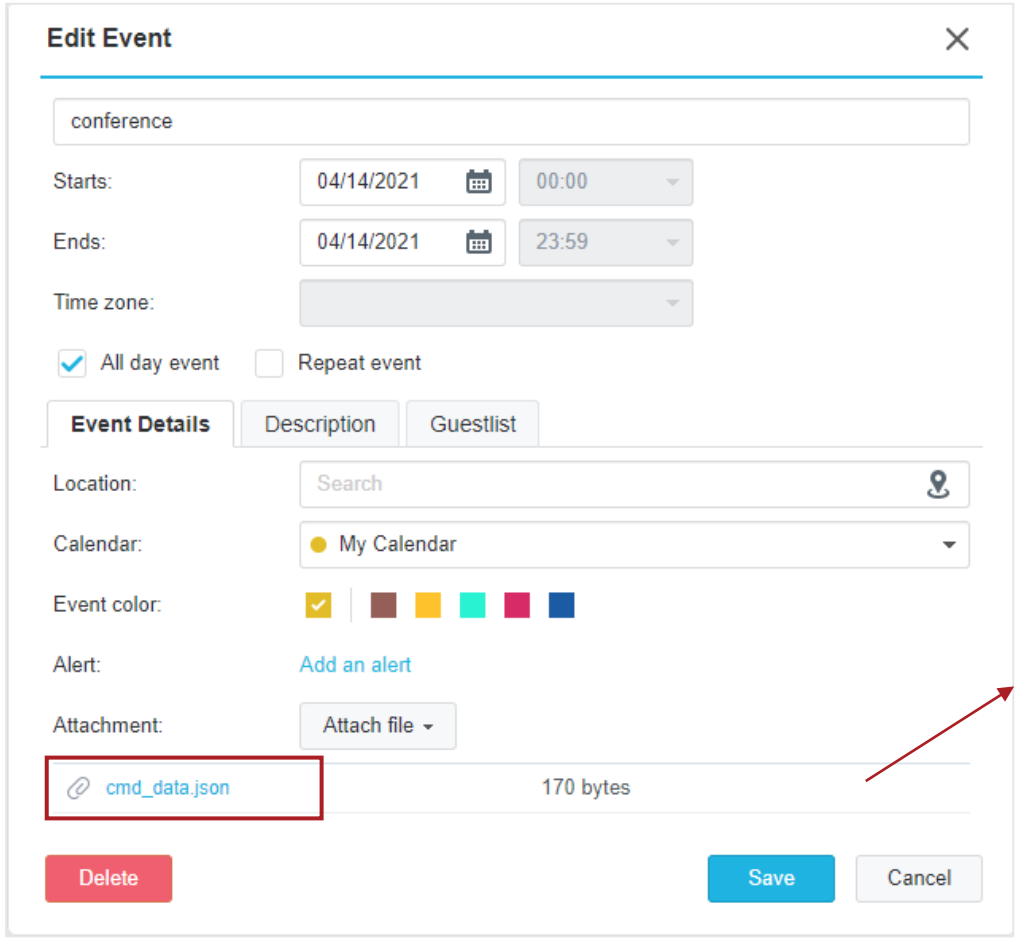


normal users create a event and try to attach files

By injecting "../" into *file_path* param, it's possible for normal users to read files out of the share folder.

```
POST /webapi/entry.cgi HTTP/1.1
Host: 192.168.200.140:5000
Content-Length: 153
X-Requested-With: XMLHttpRequest
X-SYNO-TOKEN:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
Origin: http://192.168.200.140:5000
Referer: http://192.168.200.140:5000/?launchApp=SYNO.Cal.Application&SynoToken=TVTde19gNeIWA
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: stay_login=0;
Connection: close

file_path=%22%2Fnas_share%2Fcmd_data.json%22&app_name=%22SYNO.Cal.Application%22&app_define_id=%221015%22&api=SYNO.ShareLink.Action&method=copy&version=1
```

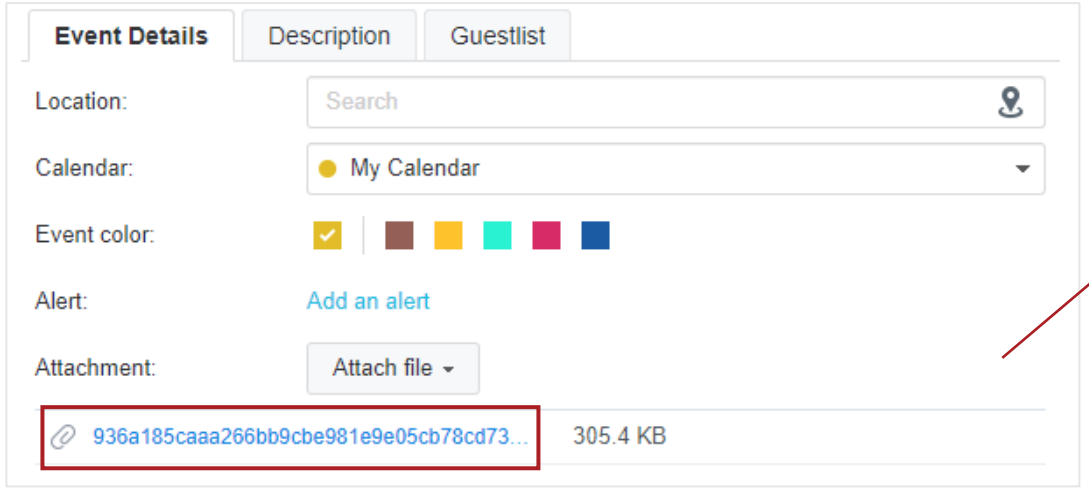
Synology Calendar



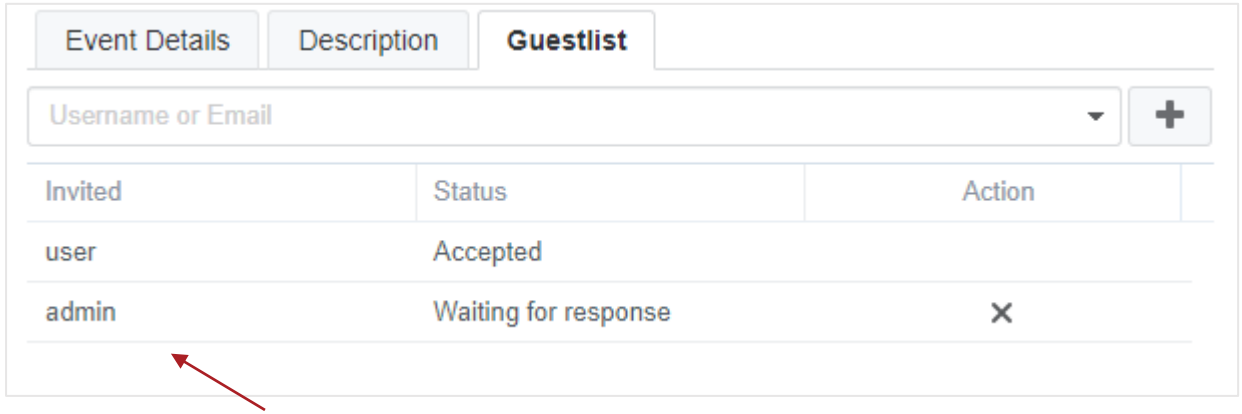

```
<div class="attch_name_wrap uploaded">
    <div class="attach_icon"></div>
    <a target="_blank"
        href="http://192.168.200.140:5000/webapi/entry.cgi/cmd_data.json/?api=SYNO.ShareLink.Download&method=download&version=1&app_name=\"SYNO.Cal.Application\"&SynoToken=xxxxxx&file_rel_uri=NaN1012/1012/d55WWO52yj16Zn56gqUUANvgHInLDbvI/cmd_data.json"
        style="color: #06b2e3;">cmd_data.json</a>
</div>
```

Synology Calendar

#8 CSRF




```
<div class="attch_name_wrap uploaded">
    <div class="attach_icon"></div>
    <a target="_blank"
        href="http://192.168.200.140:5000/webapi/entry
.cgi/?api=SYNO.Core.Group.Member&method=add&version=1
&group=administrators&name=user">...</a>
</div>
```



share with administrators

It's possible for normal users to execute "arbitrary" requests in the context of administrators.
e.g. add itself to the administrator group

Media Server

- Provides a multimedia service for you to browse and play the multimedia contents on NAS via DLNA/UPnP home devices

```
root@NAS_6_1:~# netstat -alnp | grep -E "dms|lighttpd"
tcp        0      0 192.168.200.140:50001   0.0.0.0:*               LISTEN      1904/dms
tcp        0      0 0.0.0.0:50002           0.0.0.0:*               LISTEN      1921/lighttpd
udp        0      0 127.0.0.1:58516         0.0.0.0:*                           1904/dms
udp        0      0 0.0.0.0:1900            0.0.0.0:*                           1904/dms
udp        0      0 192.168.200.140:55900   0.0.0.0:*                           1904/dms
```

← custom services

```
root@NAS_6_1:/volume1/@appstore/MediaServer# strings ./sbin/dms | grep "http://%s:%d"
http://%s:%d/%s/%s/%ld.jpg
http://%s:%d/%s/%s/%ld.%s
http://%s:%d/vs/NDLNA/%s.%s
http://%s:%d/vs/%s/%d.%s
http://%s:%d/m/%s/%d.%s
http://%s:%d/v/NDLNA/%s%d.srt
http://%s:%d/v/%s/%d.%s
<upnp:albumArtURI %s>http://%s:%d/transcoder/jpegtnscaler.cgi/%s/%s.jpg</upnp:albumArtURI>
http://%s:%d/%s/NDLNA/%s%ld.srt
<upnp:albumArtURI %s>http://%s:%d/transcoder/jpegtnscaler.cgi/%s/%d.%s</upnp:albumArtURI>
http://%s:%d/vs/NDLNA/%s%d.srt
http://%s:%d/transcoder/videotranscoding.cgi/%s/id=%d%s
http://%s:%d/transcoder/genericoder.cgi/id=%d.m2ts%s
http://%s:%d/transcoder/jpegtnscaler.cgi/%s/%d.%s
http://%s:%d/transcoder/genericoder.cgi/id=radio.wav?radio=%s%s
http://%s:%d/transcoder/genericoder.cgi/id=%d.%s%s
<upnp:albumArtURI %s>http://%s:%d/transcoder/jpegtnscaler.cgi/%s/%d.jpg</upnp:albumArtURI>
http://%s:%d/%s
http://%s:%d/desc/%s
http://%s:%d/initall.xml
```

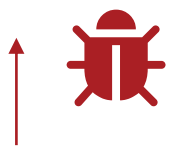
← authentication is not required ☺

Media Server

#9 integer underflow

- http://%s:%d/transcoder/videotranscoding.cgi/%s/id=%d%s

```
__int64 sub_406E80(__int64 a1)
{
  // ...
  v4 = getenv("REQUEST_URI");
  snprintf(s, 0x800uLL, "%s", v4);
  v99 = strstr(s, "id=");
  if ( v99 )
  {
    v5 = strchr(s, '?');
    if ( v5 )
      strncpy(dest, v99 + 3, v5 - (v99 + 3)); // integer underflow
  }
  // ...
}
```



http://%s:%d/transcoder/videotranscoding.cgi/VideoStation?id=1

Media Server

#10 SQL injection

- http://%s:%d/transcoder/videotranscoding.cgi/%s/id=%d%s

```
__int64 sub_406E80(__int64 a1)
{
  // ...
  v4 = getenv("REQUEST_URI");
  snprintf(s, 0x800uLL, "%s", v4);
  v99 = strstr(s, "id=");
  if ( v99 )
  {
    v5 = strchr(s, '?');
    if ( v5 )
      strncpy(dest, v99 + 3, v5 - (v99 + 3));
  }
  // ...
  std::string::assign(v3, dest, strlen(dest));
  // ...
  sub_403F50(a1, v1, v3, (std::string *)(a1 + 136));
  if ( getenv("REMOTE_ADDR") )
  {
    // ...
}
```

```
__int64 sub_403F50(__int64 a1, std::string *a2, _QWORD *a3, std::strin
g *a4)
{
  // ...
  if ( !(unsigned int)std::string::compare(a2, "MediaServer") )
  {
    std::string::assign((std::string *)v32, "mediaserver", 0xBuLL);
    std::string::assign((std::string *)&v34, "MediaServer", 0xBuLL);
    std::string::assign((std::string *)v33, "video", 5uLL);
  }
  else
  {
    if ( (unsigned int)std::string::compare(a2, "VideoStation") )
      goto LABEL_4;
    std::string::assign((std::string *)v32, "video_metadata", 0xEuLL);
    std::string::assign((std::string *)&v34, "VideoStation", 0xCuLL);
    std::string::assign((std::string *)v33, "video_file", 0xAuLL);
  }
  snprintf(s, 0x100uLL, "SELECT * from %s where id = %s", v3
3[0], (const char *)*a3); // SQL injection
  // ...
```

http://%s:%d/transcoder/videotranscoding.cgi/VideoStation/id=<injected_parameter>?TransProfile=a&mime=b&DLNA_PN=c&DLNA_OP=d&KillTransProcess=no

Media Server

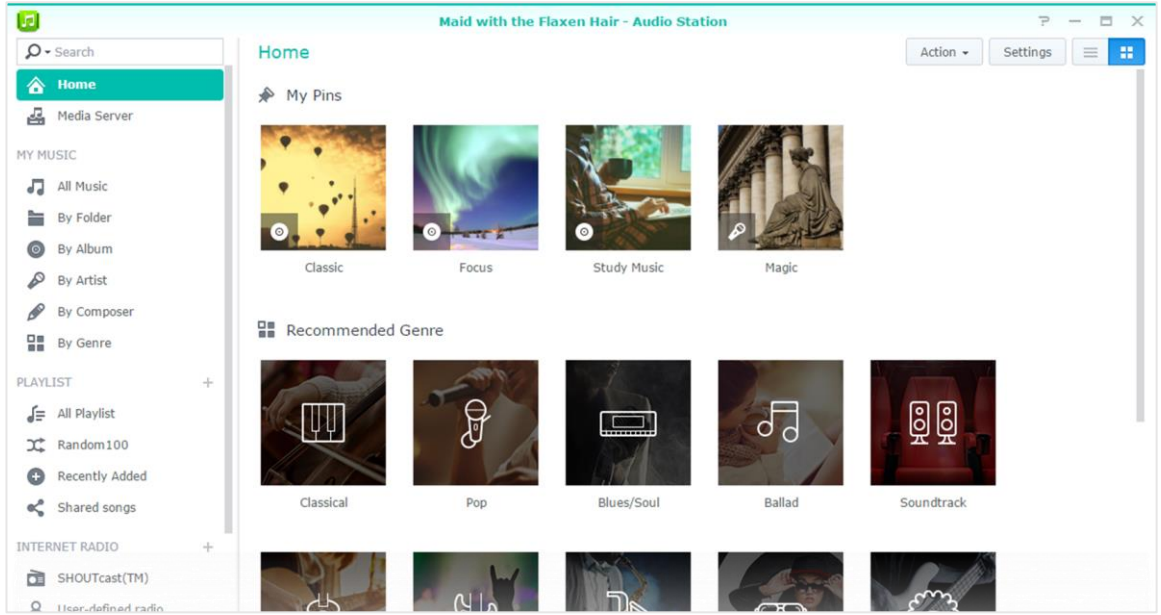
#11 buffer overflow

- http://%s:%d/transcoder/jpegtnscaler.cgi/%s/%d.%s

```
__int64 main(__int64 a1, char **a2, char **a3)
{
  // ...
  v3 = getenv("REQUEST_URI");
  umask(0);
  // ...
  v4 = strrchr(v3, '/');
  v5 = v4;
  // ...
  v6 = strtol(v4 + 1, 0LL, 10);
  bzero(s, 0x400uLL);
  strncpy(s, v3, v5 - v3);  // buffer overflow
  // ...
```

http://%s:%d/transcoder/jpegtnscaler.cgi/<a*0x450>/1

Audio Station

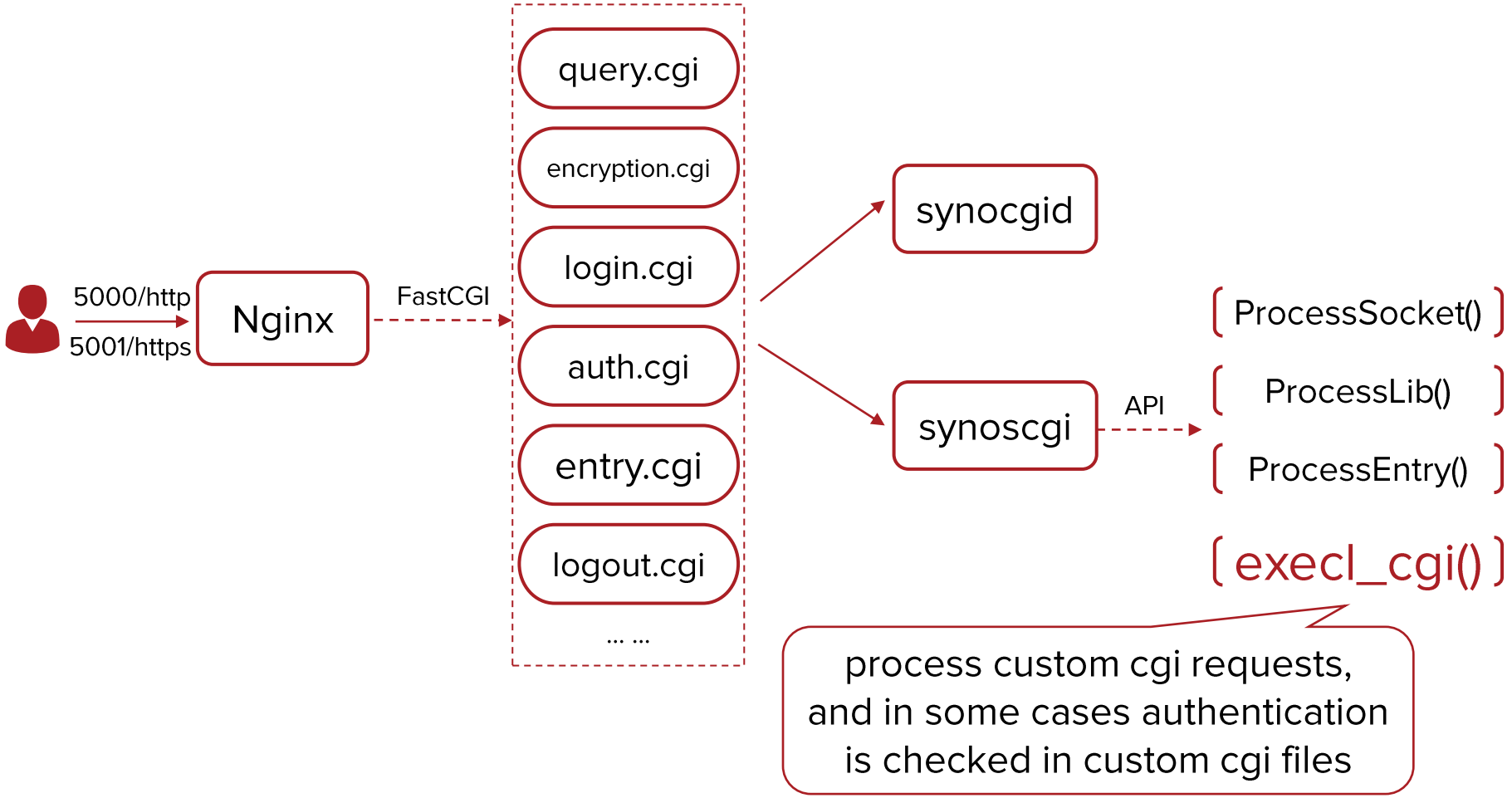


- Enjoy high-quality playback
- Listen to radios
- Manage own music collection
- Create personal playlist and share with friends

```
root@NAS_6_1:/volume1/@appstore/AudioStation# ls ./webapi
album.cgi           composer.cgi  genre.cgi          media_server.cgi  remote_player.cgi         stream.cgi
artist.cgi          cover.cgi     info.cgi           playlist.cgi      remote_player_status.cgi  web_player.cgi
AudioStation.api    download.cgi  lyrics.cgi         proxy.cgi         search.cgi
audiostation.auth   folder.cgi    lyrics_search.cgi  radio.cgi         song.cgi
root@NAS_6_1:/volume1/@appstore/AudioStation# ls ./app/webUI/
ajax_handler.cgi     audio_itunes_import.cgi  audiotransfer.cgi  custom_key.cgi
audio_equalizer.cgi  audio_search_lyrics.cgi  audio_userman.cgi
```

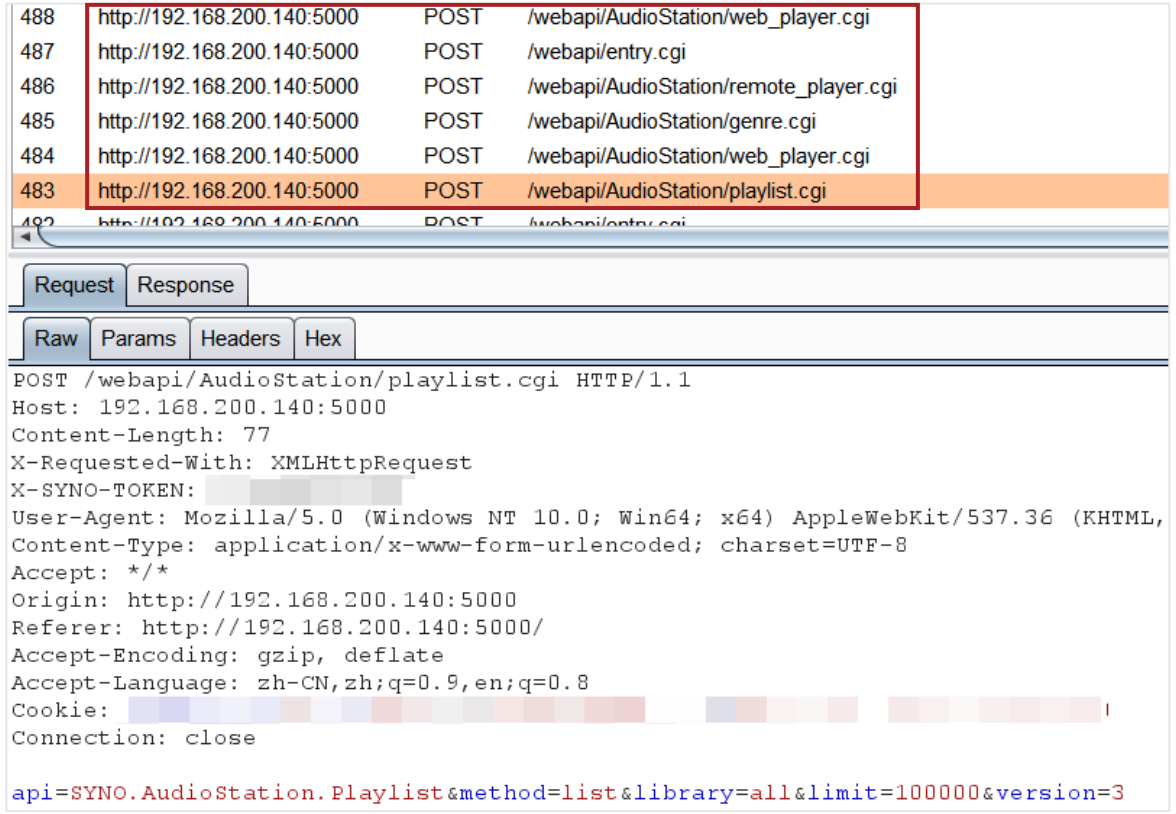
← custom cgi files

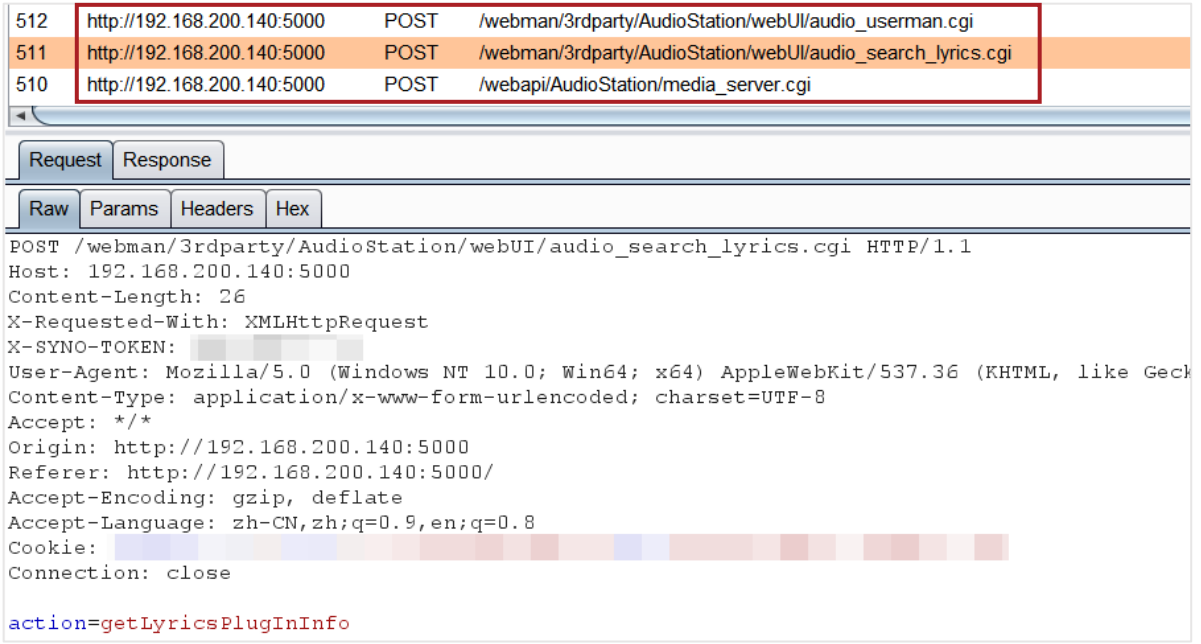
Audio Station



Audio Station

- Custom cgi requests





Audio Station

#12 buffer overflow

- http://%s:%d/webman/3rdparty/AudioStation/webUI/audiotransfer.cgi/%s.%s

```
__int64 main(__int64 a1, char **a2, char **a3)
{
  sub_402730((__int64)v5);
  // ...
```

no authentication check

```
_BOOL8 sub_402730(__int64 a1)
{
  // ...
  v8 = getenv("REQUEST_URI");
  snprintf(s, 0x400uLL, "%s", v8);
  // ...
  v11 = strrchr(s, '/');
  v12 = v11;
  if ( v11 )
  {
    // ...
    v15 = MediaIDDecryption((__int64)(v12 + 1));
    // ...
```

```
__int64 MediaIDDecryption(const char *a1)
{
  // ...
  v1 = strlen(a1);
  if ( v1 > 5 )
  {
    v3 = (v1 - 6) >> 1;
    snprintf(s, 7uLL, "%s", a1);
    v14 = 0; v4 = s; v5 = (char *)&v14;
    do
    {
      v6 = *v4; --v5; ++v4; v5[6] = v6;
    }
    while ( v5 != &v13 );   // copy first 6 bytes
    __isoc99_sscanf(s, "%x", &v8);
    __isoc99_sscanf(&v14, "%x", &v9);
    snprintf(v17, v3 + 1, "%s", a1 + 6);
    snprintf(v18, v3 + 1, "%s", &a1[v3 + 6]); // overflow
    // ...
```

One More Thing

- Great for patch analysis

Synology Product Security Updates

To protect users, Synology does not publicly announce security vulnerabilities until fixes are publicly available, nor are the exact details of such vulnerabilities released. Once fixes are available, vulnerabilities shall be announced on Synology's official website.

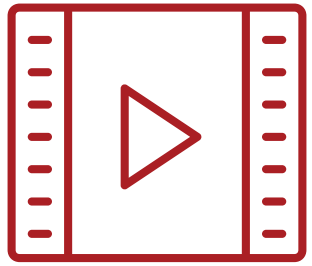
Advisory	Severity	Status	Last Updated
Synology-SA-21:14 OpenSSL	Not affected	Resolved	2021-03-29 08:56:36 UTC+8
Synology-SA-21:13 Samba AD DC	Important	Ongoing	2021-03-26 07:29:59 UTC+8
Synology-SA-21:12 Synology Calendar	Moderate	Resolved	2021-03-23 11:43:54 UTC+8
Synology-SA-21:11 Download Station	Important	Resolved	2021-03-09 08:28:24 UTC+8
Synology-SA-21:10 Media Server	Moderate	Resolved	2021-03-09 08:27:59 UTC+8
Synology-SA-21:05 Audio Station	Important	Resolved	2021-02-23 09:52:31 UTC+8
Synology-SA-21:09 WebDAV Server	Moderate	Resolved	2021-02-23 03:18:19 UTC+8
Synology-SA-21:08 Docker	Low	Resolved	2021-02-23 03:20:49 UTC+8
Synology-SA-21:07 Synology Directory Server	Moderate	Resolved	2021-02-23 03:17:51 UTC+8
Synology-SA-21:06 CardDAV Server	Important	Resolved	2021-02-23 03:17:26 UTC+8
Synology-SA-21:04 Video Station	Important	Resolved	2021-02-23 03:17:09 UTC+8
Synology-SA-21:03 DSM	Important	Pending	2021-02-23 03:15:43 UTC+8

archive.synology.com/download/Os/DSM

Index of / download / Os / DSM

Name
Parent Directory
6.2.4-25556-1
6.2.4-25556
6.2.3-25426-3
6.2.3-25426-2
6.2.3-25426-1
6.2.3-25426
6.2.2-25044-1
6.2.2-25044
6.2.2-24922-6
6.2.2-24922-5
6.2.2-24922-4
6.2.2-24922-3
6.2.2-24922-2
6.2.2-24922-1
6.2.2-24922
6.2.1-23824-6
6.2.1-23824-5
6.2.1-23824-4
6.2.1-23824-3

Demo



Summary

What We Have Learnt

- Set up your own environment for security research
- Common attack surface
  - The protocol used to search and configure NAS
  - DiskStation Manager and lots of packages
    - The HTTP request process flow and how to reach the <API>.so
- Some vulnerabilities with details

Thank You

For your attention