QNAP

In the wild QNAP NAS attacks

Genshen Ye, jinye
Aug 31, 2020 • 4 min read

Author:Yanlong Ma, Genshen Ye, Ye Jin

From April 21, 2020, 360Netlab Anglerfish honeypot started to see a new QNAP NAS vulnerability being used to launch attack against QNAP NAS equipment. We noticed that this vulnerability has not been announced on the Internet, and the attacker is cautious in the process of exploiting it.

Vulnerability analysis

Vulnerability type: Unauthorized remote command execution vulnerability

When we enter the sample into the 360 FirmwareTotal system, we found that this vulnerability appeared in the CGI program `/httpd/cgi-bin/authLogout.cgi`. This CGI is used when user logout, and it select the corresponding logout function based on the field name in the Cookie. The problem is `QPS_SID`, `QMS_SID` and `QMMS_SID` does not filter special characters and directly calls the `snprintf` function to splice `curl` command string and calls the `system` function to run the string, thus making command injection possible.

Vulnerability fix: We contacted the vendor and shared the PoC on May/13, and on Aug 12, QNAP PSIRT replied and indicated the vulnerability had been fixed in previous update but there still are devices on the network that have not been patched. We looked into the vendors' firmwares and discovered that on July 21, 2017, QNAP released firmware version 4.3.3 and this version included the fix for this vulnerability. This release replaced the `system` function with `qnap_exec`,

and the `qnap_exec` function is defined in the `/usr/lib/libuLinux_Util.so.0`. By using the `execv` to execute custom command, command injection has been avoided.

```
15    snprintf(buf2,0x101,"sid=%s",QPS_SID);
16    port = Get_Web_Access_Port();
17    snprintf(url,0x101,"http://127.0.0.1:%d/photostation/api/auth_api.php",port);
18    qnap_exec(0,0,0,"/sbin/curl","-4","--retry",0x20950,"--connect-timeout","10","-F","todo=logout",
19              "-F",buf2,"--url",url,0);
```

Attacker behavior analysis

We captured two attackers IP `219.85.109.140` and `103.209.253.252`, both use the same Payload, after successful exploits, the device will wget `http://165.227.39.105:8096/aaa` file.

So far the attacker has not implanted bot programs like regular Botnets, and the entire attack process does not seem to be fully automated. we still do not know the true purpose of the attacker yet.

On `165.227.39.105:8096`, we found two other text `.sl` and `rv`. The `.sl` file contains 2 lines.

```
IvHVFqkpELqvuN@WK
IvHVFqkpJEqr|DNWLr
```

`rv`, this file is a bash reverse shell script, the control address is `165.227.39.105`, and the port is `TCP/1234`.

When we fingerprint this host, we see that `165.227.39.105` has SSH, Metasploit, Apache httpd and other services running.

```
Discovered open port 9393/tcp on 165.227.39.105 //SSH
Discovered open port 5678/tcp on 165.227.39.105 //Unknown
Discovered open port 3790/tcp on 165.227.39.105 //Metasploit
Discovered open port 80/tcp on 165.227.39.105   //Apache httpd
```

Timeline

```
On May 13, 2020, we emailed the QNAP vendor and reported the details of the vulnerabi
On August 12, 2020, QNAP PSIRT replied that the vulnerability had been fixed in early
```

List of known affected firmware

```
HS-210_20160304-4.2.0
HS-251_20160304-4.2.0
SS-439_20160304-4.2.0
SS-2479U_20160130-4.2.0
TS-119_20160304-4.2.0
TS-210_20160304-4.2.0
TS-219_20160304-4.2.0
TS-221_20160304-4.2.0
TS-239H_20160304-4.2.0
TS-239PROII_20160304-4.2.0
TS-239_20160304-4.2.0
TS-269_20160304-4.2.0
TS-410U_20160304-4.2.0
TS-410_20160304-4.2.0
TS-412U_20160304-4.2.0
TS-419P_20160304-4.2.0
TS-419U_20160304-4.2.0
TS-420U_20160304-4.2.0
TS-421U_20160304-4.2.0
TS-439PROII_20160119-4.2.0
TS-439PROII_20160304-4.2.0
TS-439_20160304-4.2.0
TS-459U_20160119-4.2.0
TS-459U_20160304-4.2.0
TS-459_20160304-4.2.0
TS-469U_20160304-4.2.0
TS-509_20160304-4.2.0
TS-559_20160304-4.2.0
TS-563_20160130-4.2.0
TS-659_20140927-4.1.1
TS-659_20160304-4.2.0
TS-669_20160304-4.2.0
TS-809_20160304-4.2.0
TS-859U_20160304-4.2.0
TS-869_20160304-4.2.0
TS-870U_20160119-4.2.0
TS-870U_20160304-4.2.0
TS-870_20160130-4.2.0
TS-879_20160130-4.2.0
TS-1079_20160119-4.2.0
TS-1269U_20160304-4.2.0
TS-1270U_20160304-4.2.0
TS-1679U_20160304-4.2.0
TS-X51U_20160304-4.2.0
```

```
TS-X51_20160304-4.2.0
TS-X53U_20160304-4.2.0
TS-X53U_20161028-4.2.2
TS-X53U_20161102-4.2.2
TS-X53U_20161214-4.2.2
TS-X53U_20170313-4.2.4
TS-X53_20160304-4.2.0
TS-X63U_20161102-4.2.2
TS-X63U_20170313-4.2.4
TS-X80U_20160304-4.2.0
TS-X80_20160130-4.2.0
TS-X80_20160304-4.2.0
TS-X80_20161102-4.2.2
TS-X82_20161208-4.2.2
TS-X82_20170313-4.2.4
TVS-X63_20160130-4.2.0
TVS-X63_20160304-4.2.0
TVS-X63_20160823-4.2.2
TVS-X63_20160901-4.2.2
TVS-X63_20161028-4.2.2
TVS-X63_20161102-4.2.2
TVS-X63_20170121-4.2.3
TVS-X63_20170213-4.2.3
TVS-X63_20170313-4.2.4
TVS-X71U_20161208-4.2.2
TVS-X71_20160130-4.2.0
TVS-X71_20160304-4.2.0
TVS-X71_20161214-4.2.2
TVS-X71_20170313-4.2.4
```

Suggestions

We recommend that QNAP NAS users check and update their firmwares in a timely manner and also check for abnormal processes and network connections.

We recommend the following IoCs to be monitored and blocked on the networks where it is applicable.

Contact us

Readers are always welcomed to reach us on twitter, or emial to netlab at 360 dot cn.

IoC

Scanner IP

```
219.85.109.140          Taiwan                  ASN18182                Sony Network
103.209.253.252         United States           ASN33438                Highwinds Ne
```

Downloader IP

```
165.227.39.105          Canada                  ASN14061                DigitalOcean
```

URL

```
http://165.227.39.105:8096/.sl
http://165.227.39.105:8096/rv
http://165.227.39.105:8096/aaa
```

0 Comments Login ▾

G Start the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

♡ 1 Share Best Newest Oldest

Be the first to comment.

Subscribe Privacy Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —

QNAP

QNAP NAS users, make sure you check your system

QNAP NAS在野漏洞攻击事件2

QNAP NAS在野漏洞攻击事件

See all 3 posts →

honeypot

360网络安全研究院杭州开点招聘

团队简介 360网络安全研究院（360Netlab）于2014年成立。不同于传统网络安全主要基于规则，数据分析是团队的主要方向。团队持续专注于DNS和僵尸网络领域，并在领域内保持领先地位。 从2014年开始，团队在DNS方向上建设了国内历史最久、覆盖范围最广的PassiveDNS基础数据库，及其附属其它基础数据库，持续分析产出威胁情报并应用于...

Sep 8, 2020 · 6 min read

QNAP

QNAP NAS在野漏洞攻击事件

本文作者：马延龙，叶根深，金晔 背景介绍 2020年4月21号开始，360Netlab未知威胁检测系统监测到有攻击者使用QNAP NAS设备漏洞，攻击我们的Anglerfish蜜罐节点。我们看到这个漏洞PoC并没有在互联网上公布，攻击者在漏洞利用过程中相对谨慎，互联网上也仍有一些未修复漏洞的QNAP NAS设备。因此，我们需要披露这个漏洞攻击事件，并提醒安全...

Aug 31, 2020 · 5 min read