

QNAP

QNAP NAS在野漏洞攻击事件



Genshen Ye, jinye

Aug 31, 2020 • 5 min read

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，并提醒安全社区和QNAP NAS用户，避免受到此类漏洞攻击。

漏洞分析

漏洞类型：未授权远程命令执行漏洞

漏洞原因：通过360 FirmwareTotal系统分析，我们发现这个漏洞出现CGI程序 `/httpd/cgi-bin/authLogout.cgi` 中。它在处理用户注销登录时，会根据Cookie中字段名称选择相应的注销登录函数。其中 `QPS_SID`，`QMS_SID` 和 `QMMS_SID` 注销登录函数未过滤特殊字符即使用 `snprintf` 函数拼接 `curl` 命令字符串并使用 `system` 函数直接执行，所以造成命令注入。

漏洞修复：在2017年7月21号，我们发现QNAP发布固件版本4.3.3修复了这个漏洞。修复后的固件中使用 `qnap_exec` 函数替换了原来的 `system` 函数。其中 `qnap_exec` 函数在 `/usr/lib/libuLinux_Util.so.0.0` 中定义，通过调用 `execv` 函数执行自定义命令，避免命令注入。

```
15 sprintf(buf2,0x101,"sid=%s",QPS_SID);
16 port = Get_Web_Access_Port();
17 sprintf(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);
```

攻击者行为分析

我们共捕获到2个攻击者IP `219.85.109.140` 和 `103.209.253.252` 使用完全一样的Payload，漏洞攻击成功后会通过wget请求

`http://165.227.39.105:8096/aaa` 文件。

这个攻击者不像常规的Botnet一样自动化地植入Bot程序，整个攻击过程看起来也不是完全自动化执行的，根据目前的线索，我们还不清楚攻击者的真实目的。

我们在 `165.227.39.105:8096` 下载网站上发现其他2个文本文件 `.sl` 和 `rv`。其中 `.sl` 文件是2行未知的字符串。

```
IvHVFqkpELqvN@WK
IvHVFqkpJEqr|DNWLr
```

`rv` 文件是一个bash反弹shell脚本，控制地址为 `165.227.39.105`，端口为 `TCP/1234`。

此外，我们通过端口探测，发现 `165.227.39.105` 运行了SSH，Metasploit，Apache httpd等服务。

```
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
```

时间线

2020年5月13号，我们邮件联系QNAP厂商并报告了漏洞详情以及在野攻击PoC。

2020年8月12号，QNAP PSIRT联络人邮件回复该漏洞已经修复并释出安全性更新，但在网络中此类攻击仍然存在。

已知受影响固件列表

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

处置建议

我们建议QNAP NAS用户及时检查并更新固件系统，同时检查是否存在异常进程和网络连接。

我们建议读者对相关IP和URL进行监控和封锁。

联系我们

感兴趣的读者，可以在 [twitter](#) 或者通过邮件[netlab\[at\]360.cn](mailto:netlab[at]360.cn)联系我们。

IoC

Scanner IP

219.85.109.140
103.209.253.252

Taiwan
United States

ASN18182
ASN33438

Sony Network
Highwinds Net

Downloader IP

URL

<http://165.227.39.105:8096/.sl>
<http://165.227.39.105:8096/rv>
<http://165.227.39.105:8096/aaa>

— 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

In the wild QNAP NAS attacks

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

In the wild QNAP NAS attacks

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



Aug 31,

4 min



2020

read

