

QNAP

QNAP NAS在野漏洞攻击事件2



Ma Yanlong, Genshen Ye

Mar 5, 2021 • 6 min read

背景介绍

2021年3月2号，360网络安全研究院未知威胁检测系统监测到攻击者正在使用台湾QNAP Systems, Inc.公司的网络存储设备诊断程序(Helpdesk)的未授权远程命令执行漏洞（CVE-2020-2506 & CVE-2020-2507），获取到系统root权限并进行恶意挖矿攻击。

我们将此次挖矿程序命名为UnityMiner，值得注意的是攻击者专门针对QNAP NAS设备特性，隐藏了挖矿进程，隐藏了真实的CPU内存资源占用信息，使用户无法在Web管理界面看到系统异常行为。

2020年10月7号，QNAP Systems, Inc.公司发布安全公告QSA-20-08[\[1\]](#)，并指出已在Helpdesk 3.0.3和更高版本中解决了这些问题。

目前，互联网上还没有公布CVE-2020-2506和CVE-2020-2507的漏洞详细信息，由于该漏洞威胁程度极高，为保护尚未修复漏洞的QNAP NAS用户，我们不公开该漏洞技术细节。我们推测仍有数十万个在线的QNAP NAS设备存在该漏洞。

此前我们曾披露了另一起QNAP NAS在野漏洞攻击事件[\[2\]](#)。

注意：该攻击事件仍在进行中，攻击者具备优质的1-day漏洞资源，并根据QNAP设备特性定制化开发。

漏洞影响范围

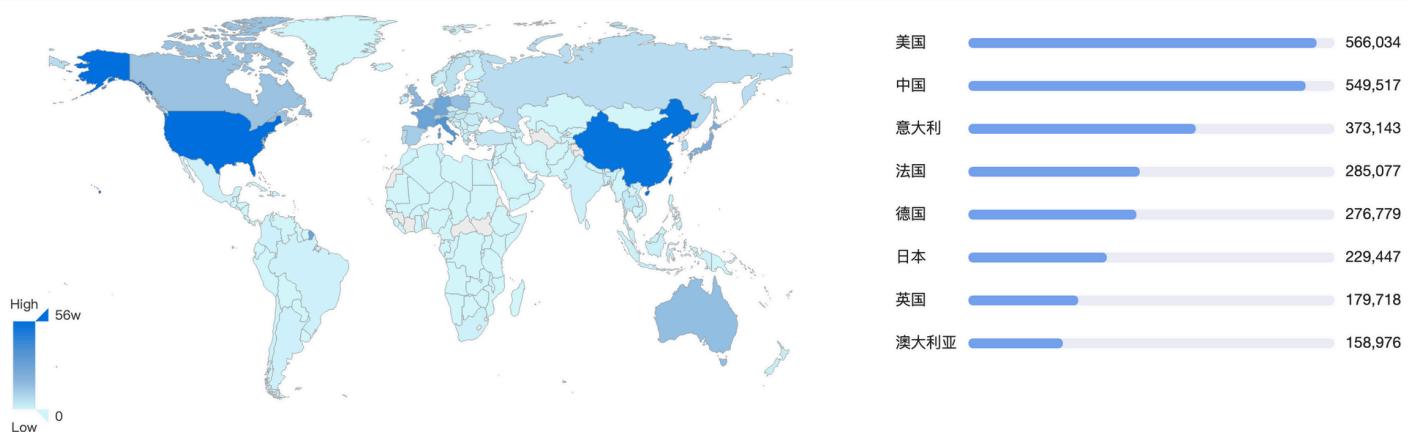
360 FirmwareTotal系统通过对QNAP NAS固件分析和漏洞验证，发现2020年8月以前的固件均受该漏洞影响，以下是已知固件列表。

TVS-X73
TVS-X71U
TVS-X71
TVS-X63
TS-XA82
TS-XA73
TS-XA28A
TS-X89U
TS-X88
TS-X85U
TS-X85
TS-X83XU
TS-X82U
TS-X82S
TS-X82
TS-X80U
TS-X80
TS-X77U
TS-X77
TS-X73U
TS-X72U
TS-X72
TS-X63U
TS-X53U
TS-X53S
TS-X53D
TS-X53BU
TS-X53B
TS-X53A
TS-X53
TS-X51U
TS-X51DU
TS-X51B
TS-X51A
TS-X51
TS-X35A
TS-X28A
TS-KVM
TS-879U
TS-879
TS-870U
TS-870
TS-869U
TS-869
TS-859U
TS-859
TS-809U

TS-809
TS-670
TS-669
TS-659
TS-639
TS-569
TS-559
TS-509
TS-470
TS-469U
TS-469
TS-459U
TS-459
TS-439U
TS-439PROII
TS-439
TS-421U
TS-421
TS-420U
TS-420
TS-419U
TS-419P
TS-412U
TS-412
TS-410
TS-269
TS-259
TS-239PROII
TS-239H
TS-239
TS-221
TS-220
TS-219
TS-212
TS-210
TS-1679U
TS-1279U
TS-1270U
TS-1269U
TS-121
TS-120
TS-119
TS-112
TS-110
TS-1079
SS-839
SS-439
SS-2479U
SS-1879U
SS-1279U
QGD-1600
Mustang-200
IS-400

360 Quake网络空间测绘系统通过对全网资产测绘，发现QNAP NAS共4297426条数据记录，其中有951486个独立IP，设备具体分布如下图所示。

世界数据统计



挖矿套件简析

1. 概况

挖矿套件由 **unity_install.sh** 和 **Quick.tar.gz** 组成，**unity_install.sh** 用来下载&设置&启动挖矿程序，并劫持原设备中的 **manaRequest.cgi** 程序；**Quick.tar.gz** 中则打包了矿机程序、矿机配置文件、矿机启动脚本和伪造的 **manaRequest.cgi**：

```
Quick
├── config.json
├── manaRequest.cgi
├── start.sh
└── unity
```

其中 **unity** 为 XMRig 矿机程序，因此暂时将此挖矿套件命名为 **UnityMiner**。

2. **unity_install.sh**

核心功能：

- 检查是否存在旧的 **unity** 进程，存在则 Kill 掉 **unity** 进程
- 检查设备 CPU 架构，下载相应的挖矿套件，支持 ARM64 和 AMD64 两种 CPU 架构

- 根据 CPU 核数设置 config.json 中的挖矿参数（用半数的 CPU 核来挖矿）
- 解压矿机套件，设置 cron 并执行挖矿脚本 `start.sh`（每分钟执行一次，时间间隔设置为 `* * * * *`）

3. start.sh

核心功能：

- 检查 `unity` 进程，不存在则启动本地 `unity` 挖矿程序；
- 把系统文件 `/home/httpd/cgi-bin/management/manaRequest.cgi` 重命名为 `manaRequests.cgi`（该文件负责设备系统信息的查看和修改，参考 [通过API取得和修改nas的信息demo程序](#)）
- 把 `Quick.tar.gz` 中的 `manaRequest.cgi` 文件复制到 `/home/httpd/cgi-bin/management/` 目录中，替换系统自身的同名文件。

4. config.json

该团伙用自己搭建的 Pool(Proxy)，所以无法看到真实的 XMR Wallet。挖矿配置共 3 组，`user` 都是 `"xmr2"`，`pass` 都是 `"x"`，Pool(Proxy) 分别如下：

```
aquamangts.tk:12933
a.aquamangts.tk:12933
b.aquamangts.tk:12933
```

5. manaRequest.cgi

核心功能：

- 劫持系统的原同名文件，收到 HTTP 请求后，先检测系统中是否存在 `unity` 挖矿进程，如果不存在，则直接把 HTTP 请求转给系统原同名文件（已被重命名为 `manaRequests.cgi`）处理，之后结束执行：

```
count=`ps -fe | grep unity | grep -v "grep"`
if [ "" == "$count" ];then
    /home/httpd/cgi-bin/management/manaRequests.cgi
```

```
    exit 0  
fi
```

- 如果系统中存在 `unity` 挖矿进程，则在把 HTTP 请求转给系统原同名文件执行后，把执行的结果记录下来(存放到 `.log.log` 文件中)，然后篡改执行结果：
 - 把 CPU 状态数据(usage 和 tempc) 都减去 50
 - 删除执行结果中 `unity` 进程信息

之后，伪造的 `manaRequest.cgi` 会把真实的 `manaRequest.cgi` 执行后篡改的数据，以 `cat .log.log` 的方式返回给请求方，这样系统管理界面就不会从设备信息中发现异常，从而达到隐藏挖矿进程的目的。

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**联系我们。

IoC

IP:

210.201.136.170

Taiwan

ASN9311

HITRON TECHNO

Miner Proxy:

aquamangts.tk:12933
a.aquamangts.tk:12933
b.aquamangts.tk:12933

URL:

```
http://c.aquamangts.tk:8080/QFS/install/unity_install.sh  
http://c.aquamangts.tk:8080/QFS/arm64/Quick.tar.gz  
http://c.aquamangts.tk:8080/QFS/amd64/Quick.tar.gz
```

MD5:

```
0f40086c9e96c9c11232a9175b26c644  
1eb01a23a122d077540f83b005abdbfc  
97015323b4fd840a40a9d40d2ad4e7af
```

招聘信息

360网络安全研究院在杭州新成立了一个产品团队，把我们的安全数据和技术产品化，探索网络安全行业未知威胁检测难题，为360安全大脑添砖加瓦。

从一次平凡的网络扫描，到漏洞、样本、安全事件分析，再到0-day漏洞检测、未知恶意软件检测、高级威胁追踪，我们致力于通过数据驱动安全，构建网络安全看得见的能力。

招聘岗位：

前端开发工程师、后端开发工程师、产品经理、安全工程师、算法工程师

详情链接：<https://blog.netlab.360.com/work-in-hangzhou/>



QNAP NAS users, make sure you check your system

QNAP NAS在野漏洞攻击事件

In the wild QNAP NAS attacks

[See all 3 posts →](#)

check your system

Background On March 2, 2021, 360Netlab Threat Detection System started to report attacks targeting the widely used QNAP NAS devices via the unauthorized remote command execution vulnerability (CVE-2020-2506 & CVE-2020-2507)[1], upon successful attack, the attacker will gain root privilege on the device and...



Mar 5,

4 min



2021

read

级“武器库”

版权 版权声明: 本文为Netlab原创, 依据CC BY-SA 4.0 许可证进行授权, 转载请附上出处链接及本声明。概述 自2021年2月15号起, 360Netlab的BotMon系统持续检测到Gafgyt家族的一个新变种, 它使用Tor进行C2通信以隐藏真实C2, 并对样本中的敏感字符串做了加密处理。这是我们首次发现使用Tor机制的Gafgyt变种, 所以将该变种命名为Gafgyt_tor。...



• Mar 5, 2021 • 15 min read