UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00120

## QNAP NAS SUSCEPTIBLE TO CRYPTOMINING

**DATE ISSUED:** 15th March 2021

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | HIGH |
| EASE OF EXPLOIT | HARD | MEDIUM | EASY |

## OVERVIEW

After patching a critical vulnerability in October 2020, QNAP have been notified in a surge of attacks taking advantage of unpatched devices affecting over 100 versions of the firmware to mine cryptocurrencies.

## BREAKDOWN

All versions prior to the 3.0.3 Helpdesk firmware for QNAP are affected by two bugs, the first of which is an improper-acccess-control tracked as CVE-2020-2506, and the second is a command injection vulnerability tracked as CVE-2020-2507. 360 Netlab have dubbed the novel cryptomining malware "UnityMiner" which is able to hide its activity from administrators who log in to check system usage and CPU memory allocation. The executable file unity_install.sh (the initiator) and Quick.tar.gz (containing the miner program) are used to install the mining software and hijack the manaRequest.cgi program using a file forgery. It then uses the Helpdesk processes to rename and commandeer the system file /home/httpd/cgi-bin/management/manaRequest.cg which under normal circumstances allows system monitoring, thus obscuring its activities. The attackers then establish their own proxy pools to hide their cryptocurrency wallet which stores the harvested Monero cryptocurrency.

## REMEDIATION STEPS

- Update all QNAP Network Attached Storage (NAS) devices with versions prior to 3.0.3

## REFERENCES & RESOURCES


| | |
|---|---|
| Sophos | https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/Cryptomining-malware-on-NAS-servers.pdf |
| Threatpost | https://threatpost.com/miner-campaign-targets-unpatched-qnap-nas/164580/ |
| ZDNet | https://www.zdnet.com/article/pycryptominer-enslaves-your-pc-to-mine-monero/ |
| Tom's Hardware | https://www.tomshardware.com/news/hackers-exploit-qnap-vulnerabilities-turn-nas-crypto-miners |