UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
🌐 www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00141

URGENT SECURITY UPDATE: QNAP NAS

DATE ISSUED: 30th April 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

QNAP NAS (Network Attached Storage) is under active exploitation whereby ransomware (Qlocker and eCh0raix) is being deployed running the QTS operating system or a variety of add-ons.

BREAKDOWN

Affected devices will experience mass file encryption with a .7z suffix that requires a password for access and to be decrypted. A ransom note will also be present under the label "!!!READ_ME.txt". Affected devices include:

- Hybrid Backup Sunc versions before: 16.0.0415 for QTS 4.5.x, 3.0.210412 for QTS 4.3.x, 16.0.0419 for QuTS hero and QuTScloud
- Media Streaming add-on versions before: 430.1.8.10
- Multimedia consoles before 1.3.4
- QTS versions before: 4.5.2.1566 Build 20210202, 4.3.6.1620 Build 20210322, 4.2.6 Build 20210327, QuTS her h4.5.1.1491 build 20201119

REMEDIATION STEPS

- Ensure the device is not exposed to the internet, particularly the web interface or file shares – change default web port 8080.
- Use QNAP resources listed below for comprehensive remediation actions and tools.
- All QNAP devices require updates according to the instructions from QNAP.
- Contact QNAP technical support for further enquiries at https://service.qnap.com
- Report any incidents of breach to CERT NZ by calling 0800 CERTNZ or via their website https://www.cert.govt.nz/it-specialists/report-an-incident

REFERENCES & RESOURCES

CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/qnap-nas-vulnerabilities-exploited-to-deploy-ransomware/
QNAP	What to do is NAS is encrypting my files https://bit.ly/3tebl1f Response to Qlocker ransomware actions https://bit.ly/3xJoYZN Best Practices for securing NAS https://bit.ly/3eEJUZa