TLP: White[1]

Ransomware attack on QNAP NAS Devices

Dear Constituents,

A new ransomware strain called "Qlocker" is targeting QNAP network attached storage (NAS) devices as part of an ongoing campaign and encrypting files in password-protected 7zip archives. It was confirmed that the Qlocker ransomware is exploiting one of the patched HBS vulnerabilities against unpatched QNAP NAS that are directly connected to the Internet.

How it works

The attacker took advantage of a patched (Hybrid Backup Sync) HBS vulnerability.

1. Once the weakness is exploited, the malware could obtain the inappropriate permission level of the QNAP NAS involved.
2. After the NAS is breached, the attacker would insert malicious code into the system to delete all snapshots and to compress user files with a password by using the built-in 7-Zip utility that is intended for normal file compression/decompression operations.
3. After the encryption begins, Qlocker will leave a ransom note and delete itself to increase the difficulty for investigation.

What to do

- Ensure to immediately install the latest Malware Remover version and run a malware scan on QNAP NAS. The Multimedia Console, Media Streaming Add-on, and Hybrid Backup Sync apps need to be updated to the latest available version as well to further secure QNAP NAS from ransomware attacks.
- It is strongly recommended that users do not directly connect the QNAP NAS to the Internet. This is to enhance the security of your QNAP NAS device.
- It is also recommended to all users to enable the VPN server service on their router. To access your QNAP NAS from the Internet:

1 CERT Tonga adopts the Traffic Light Protocol

- first establish a VPN connection to your router
- Then connect to the QNAP NAS via VPN. This can effectively harden the NAS and decrease the chance of being attacked.

Reference

- https://www.qnap.com/static/landing/2021/qlocker/response/en/
- https://www.qnap.com/en/security-news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas

For more information please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
Email: cert@cert.gov.to
Web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga