U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00185

NEW RANSOMWARE TARGETS NAS DEVICES

DATE ISSUED: 16th August 2021

IMPACT	LOW	MEDIUM	▼ HIGH
EASE OF EXPLOIT	HARD	MEDIUM ▼	EASY

OVERVIEW

A ransomware variant known as eCh0raix (AKA QNAPCrypt) that has been in circulation for the past nine years targeting QNAP NAS devices – commonly used in Small Office and Home Office (SOHO) setups can now target QNAP and Synology devices in one attack.

BREAKDOWN

Targeting the Network Attached Storage (NAS) devices this new variant is able to hit both it's targeted vendor devices in one go. Palo Alto released a report detailing the exploitation of the vulnerability CVE-2021-28799 which leverages improper authorisation. What this means is attackers are able to gain access to hard-coded credentials and establish a backdoor, giving them free access to the devices to deploy the ransomware. There are no known reported cases of Synology devices being targeted at this stage. The new variant is compiled in GoLang and the project name is "rct_cryptor_universal" (/home/dev/GoglandProjects/src/rct_cryptor_universal).

REMEDIATION STEPS

- Update device firmware on all NAS devices .
- Use complex passwords to prevent brute-force password cracking.
- To prevent network attacks, limit connections to NAS devices from only a hard-coded list of recognized IP addresses.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/ech0raix-ransomware-variant-qnap-synology-nas-devices/168516/
Palo Alto Unit 42	https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/
QNAP	https://www.qnap.com/en-us/security-advisory/qsa-21-13