UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00254

‘DIRTY PIPE’ LINUX FLAW AFFECTS QNAP NAS

DATE ISSUED: 22nd March 2022

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

QNAP’s manufacturer has issued a warning about a Linux kernel flaw known as ‘Dirty Pipe’ that allows root access to an unprivileged user with local access affects a vast majority of their Network Attached Storage (NAS) appliances.

BREAKDOWN

This high-severity local privilege escalation vulnerability affects the Linux kernel present on all QNAP NAS running QTS 5.0.x and QuTS hero 5.0.x on all x86-based NAS and some ARM-based NAS, which allows a user with access to gain admin rights to perform attacks such as the injection of malicious code. This is made possible by the overwriting of data in arbitrary read-only file leading to privilege escalation due to a “flaw in the way the way the ‘flags’ member of the new pipe buffer structure was lacking proper initialisation in copy_page_to_iter_pipe and push_pipe functions.”

Devices running QTS 4.x and those running Linux kernel 5.10.102, 515.25 & 5.16.11 and above are unaffected. QNAP have issued a statement to say there are currently no mitigations available for the vulnerability as of March 14, 2022 but QNAP have advised they are currently working on a security patch. It is currently being tracked as CVE-2022-0847. The Linux new site Linuxiac have commented that as Linux is the base for Android devise, those running version 5.8 or later may also be vulnerable, particularly noting the new Samsung Galaxy S22 which runs 5.10.43.

REMEDIATION STEPS

- Presently there are no mitigations or patches available. Monitor vendor sites and comms channels to stay informed when patches are released and install immediately.
- Ensure only those people and systems that require access are granted it.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/most-qnap-nas-devices-affected-by-dirty-pipe-linux-flaw/178920/
QNAP	https://www.qnap.com/en-us/security-advisory/qsa-22-05
	https://www.qnap.com/en-us/release-notes/kernel
Max Kellerman	https://dirtypipe.cm4all.com/