LATERAL SECURITY

Lateral Security

Remote Code Execution in QNAP QTS

Security Advisory

CVE-2017-10700

30 August 2017

Technical Advisory

Issue Background

QNAP Systems, Inc. is a Taiwanese corporation that specializes in providing networked solutions for file sharing, virtualization, storage management and surveillance applications to address corporate, SMB, SOHO and home user needs. The QTS firmware is developed by QNAP and distributed for use on their network devices. This software provides operating system, file sharing, multimedia, surveillance, productivity and extensibility to QNAP devices.

The QNAP QTS firmware exposes a suite of media library functions. This media library service can scan multimedia files, such as photos, music and videos from designated media folders and index them into the media library for their display in multimedia applications.

The media library service fails to sufficiently sanitise user inputs. A remote, un-authenticated attacker can provide inputs to this service which executes system commands in the context of the "admin" user of the QNAP device. The admin user holds root privileges on the device.

CVSS

Base Score: 10 (Critical)

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:R

Exploitation

At the request of QNAP, a proof of concept exploit for this vulnerability is scheduled for release on 30/09/2017.

Tested Software Release

QNAP QTS version 4.3.3.0229. Prior versions may also be vulnerable.

Known Mitigations

Patch to the latest QNAP QTS firmware version. Disabling the media library component does not mitigate this vulnerability.

Researcher

Adam Bell

Timeline

30/06/2017 – Issue reported to QNAP
01/07/2017 – CVE-2017-10700 allocated by Mitre
04/07/2017 – Issue acknowledged by QNAP
28/07/2017 – QNAP release QTS 4.3.3.0262 to resolve issue
30/08/2017 – Initial public disclosure
30/09/2017 – Intended full public disclosure