Advisory Alert

Alert Number: AAA20230925 **Date:** September 25, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**High**, **Medium**	Multiple vulnerabilities

Description

Affected Product	**Qnap**
Severity	**High** , **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-23364, CVE-2023-23363, CVE-2006-20001, CVE-2022-36760, CVE-2022-37436)
Description	Qnap has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could lead to remote code execution, Buffer Overflow , HTTP Request/Response Splitting. Qnap recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	Multimedia Console version prior to 2.1.1 Multimedia Console version prior to 1.4.7 QTS 4.3.6.2441 build version prior to 20230621 QTS 4.3.4.2451 build version prior to 20230621 QTS 4.3.3.2420 build version prior to 20230621 QTS 4.2.6 build version prior to 20230621 QTS 5.1.0.2348 build version prior to 20230325 QuTS hero h5.1.0.2392 build version prior to 20230508 QuTScloud version prior to c5.0.1.2374
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-12 https://www.qnap.com/en/security-advisory/qsa-23-25 https://www.qnap.com/en/security-advisory/qsa-23-29

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.