Advisory Alert

Alert Number: AAA20240909 **Date:** September 9, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**High**, **Medium**	Multiple Vulnerabilities
Synology	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Qnap**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21906, CVE-2024-32763, CVE-2024-38641, CVE-2023-34974, CVE-2023-34979, CVE-2024-32771, CVE-2023-39298, CVE-2023-38545, CVE-2023-39300)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Arbitrary Code Execution, Bruce Force attacks, Privilege Escalation, Information Disclosure. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS 5.1.x, 4.5.x, QTS 4.3.6, QTS 4.3.4, QTS 4.3.3, QTS 4.2.6 QuTS hero h5.1.x, h4.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-24-33 • https://www.qnap.com/en/security-advisory/qsa-24-32 • https://www.qnap.com/en/security-advisory/qsa-24-28 • https://www.qnap.com/en/security-advisory/qsa-24-27 • https://www.qnap.com/en/security-advisory/qsa-24-26

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Synology has released security updates addressing multiple vulnerabilities that exist in Synology Router Manager. These vulnerabilities allow remote authenticated users to inject arbitrary web script or HTML via a susceptible version of SRM. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Synology Router Manager (SRM) version 1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_24_09

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.