Advisory Alert

Alert Number: AAA20240205 **Date:** February 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Qnap	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NetApp	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Qnap**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39302, CVE-2023-39303, CVE-2023-41273, CVE-2023-41274, CVE-2023-41275, CVE-2023-41276, CVE-2023-41277, CVE-2023-41278, CVE-2023-41279, CVE-2023-41280, CVE-2023-41292, CVE-2023-45035, CVE-2023-45036, CVE-2023-45037, CVE-2023-45025, CVE-2023-39297, CVE-2023-41281, CVE-2023-41282, CVE-2023-41283, CVE-2023-32967, CVE-2023-45026, CVE-2023-45027, CVE-2023-45028, CVE-2023-47564, CVE-2023-47566, CVE-2023-47567, CVE-2023-47568, CVE-2023-48795, CVE-2023-50359)
Description	Qnap has released security updates addressing Multiple Vulnerabilities that exist in their products. Successful exploitation of the above vulnerabilities could lead to denial-of-service (DoS), command execution, access restriction bypass, sensitive data exposure, modification and reading of critical resources. Qnap recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Qsync Central 4.3.x, 4.4.x QTS 4.5.x, 5.1.x QuTS hero h4.5.x QuTS hero h5.1.x QuTScloud 5.x, c5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/go/security-advisory/qsa-24-07 https://www.qnap.com/go/security-advisory/qsa-24-06 https://www.qnap.com/go/security-advisory/qsa-24-05 https://www.qnap.com/go/security-advisory/qsa-24-04 https://www.qnap.com/go/security-advisory/qsa-24-03 https://www.qnap.com/go/security-advisory/qsa-24-02 https://www.qnap.com/go/security-advisory/qsa-24-01 https://www.qnap.com/go/security-advisory/qsa-23-53 https://www.qnap.com/go/security-advisory/qsa-23-47 https://www.qnap.com/go/security-advisory/qsa-23-46 https://www.qnap.com/go/security-advisory/qsa-23-38 https://www.qnap.com/go/security-advisory/qsa-23-33 https://www.qnap.com/go/security-advisory/qsa-23-30

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-27318)
Description	NetApp has released a security update addressing a Denial of Service (DoS) vulnerability that exists in StorageGRID (formerly StorageGRID Webscale). A successful exploit could lead to a crash of the Local Distribution Router (LDR) service. NetApp recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 - 11.6.0.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240202-0012/

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.