Multiple Vulnerabilities in QNAP NAS

Severity Level: High

Components Affected

- QTS version prior to 5.1.3.2578 build 20231110
- QuTS hero version prior to h5.1.3.2578 build 20231110

Overview

Multiple vulnerabilities were identified in QNAP NAS, where a remote attacker could exploit some of these vulnerabilities to trigger denial of service condition, remote code execution and data manipulation on the targeted system.

Description

Multiple vulnerabilities have been discovered in QNAP NAS, introducing serious security risks. These vulnerabilities could be exploited remotely by a malicious attacker to launch various types of attacks, including triggering a denial of service condition, executing arbitrary code from a remote location, and manipulating data on the targeted QNAP NAS system. Users and administrators are strongly advised to promptly apply patches and updates provided by QNAP, review and adjust system configurations, implement network security measures, monitor for suspicious activities, and educate users on security best practices to mitigate the identified risks and enhance the overall security posture of QNAP NAS devices.

Impact

- Remote Code Execution
- Denial of Service
- Data Manipulation

Solution/ Workarounds

- Apply fixes issued by the vendor by updating to the latest version.

Reference

- https://www.qnap.com/en/security-advisory/qsa-23-64

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.