Severity

Medium

Analysis Summary

CVE-2021-34360

QNAP NAS is vulnerable to cross-site request forgery, caused by improper validation of user-supplied input by the Proxy Server. By persuading an authenticated user to visit a malicious Web site, a remote attacker could send a malformed HTTP request to perform unauthorized actions. An attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities.

Impact

- Unauthorized Access

Indicators Of Compromise

CVE

- CVE-2021-34360

Affected Vendors

- QNAP

Affected Products

- QNAP QTS 4.5.x Proxy Server 1.4.2
- QNAP QTS 5.0.x Proxy Server 1.4.2
- QNAP QuTS hero h5.0.x Proxy Server 1.4.3
- QNAP QuTScloud c4.5.x Proxy Server 1.4.2

Remediation

Refer to QNAP Security Bypass for patch, upgrade, or suggested workaround information.

QNAP Security Bypass