Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

QNAP Flaws Enable Remote Code Execution Under Certain Conditions

Date of Publication	Admiralty Code	TA Number
May 22, 2024	A1	TA2024199

Summary

Discovered: May 2024
Affected Products: QTS and QuTS hero
Impact: Multiple vulnerabilities have been reported that affect certain versions of the QNAP operating system. One of these vulnerabilities, CVE-2024-27130, is an unauthenticated stack overflow vulnerability for which a proof-of-concept has been released. This vulnerability may be exploited for remote code execution, posing a significant security risk to affected systems.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-27130	QNAP QTS/QuTS hero Buffer Overflow Vulnerability	QTS and QuTS hero	✗	✗	✓
CVE-2024-21902	QNAP QTS/QuTS hero Permission Assignment Vulnerability	QTS and QuTS hero	✗	✗	✓
CVE-2024-27127	QNAP QTS/QuTS hero Double Free Vulnerability	QTS and QuTS hero	✗	✗	✓
CVE-2024-27128	QNAP QTS/QuTS hero Buffer Overflow Vulnerability	QTS and QuTS hero	✗	✗	✓
CVE-2024-27129	QNAP QTS/QuTS hero Buffer Overflow Vulnerability	QTS and QuTS hero	✗	✗	✓

Vulnerability Details

#1 Multiple vulnerabilities have been reported that affect certain versions of QNAP operating systems. Among these, a proof-of-concept has been released for one particularly critical issue: an unauthenticated stack overflow vulnerability (CVE-2024-27130). This vulnerability can be exploited for remote code execution, posing a significant security risk.

#2 The QNAP CVE-2024-27130 vulnerability is a security flaw resulting from the unsafe use of the 'strcpy' function in the No_Support_ACL function, which is part of the share.cgi script used for sharing media with external users. An attacker can exploit this vulnerability by crafting a malicious request with a specially crafted 'name' parameter, leading to a buffer overflow and remote code execution.

#3 To exploit this vulnerability, an attacker needs a valid 'ssid' parameter, which is generated when a NAS user shares a file from their QNAP device. This parameter is included in the URL of the 'share' link and can potentially be obtained through social engineering. Although not straightforward to exploit, the SSID prerequisite can be met by certain actors.

#4 QNAP operating systems have been identified with several other code execution vulnerabilities, including CVE-2024-27127, CVE-2024-27128, and CVE-2024-27129. Additionally, another flaw, CVE-2024-21902, allows authenticated users to read or modify resources via a network. Administrators are advised to regularly update their systems to mitigate the risk of exploitation of these vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-27130	QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7	cpe:2.3:a:qnap:qts:*:*:*:*:*:*:*:* cpe:2.3:a:qnap:quts_hero:*:*:*:*:*:*:*:*	CWE-121
CVE-2024-21902	QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7		CWE-200
CVE-2024-27127	QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7		CWE-415
CVE-2024-27128	QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7		CWE-121
CVE-2024-27129	QTS Prior to 5.1.7 and QuTS hero Prior to h5.1.7		CWE-121

Recommendations

Update: Admins are advised to update their QNAP systems to the latest versions to mitigate the risk of exploitation of these and other vulnerabilities. Specifically, update to:
QTS 5.1.7.2770 build 20240520 or later
QuTS hero h5.1.7.2770 build 20240520 or later

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0040 Impact	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1203 Exploitation for Client Execution	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation
T1070 Indicator Removal	T1495 Firmware Corruption	T1190 Exploit Public-Facing Application	T1135 Network Share Discovery

Patch Details

Admins are advised to update their QNAP systems to the latest versions to mitigate the risk of exploitation of these and other vulnerabilities.
QTS 5.1.7.2770 build 20240520 or later
QuTS hero h5.1.7.2770 build 20240520 or later

Links:
https://www.qnap.com/en-in/download

References

https://www.qnap.com/en/security-advisory/qsa-24-23

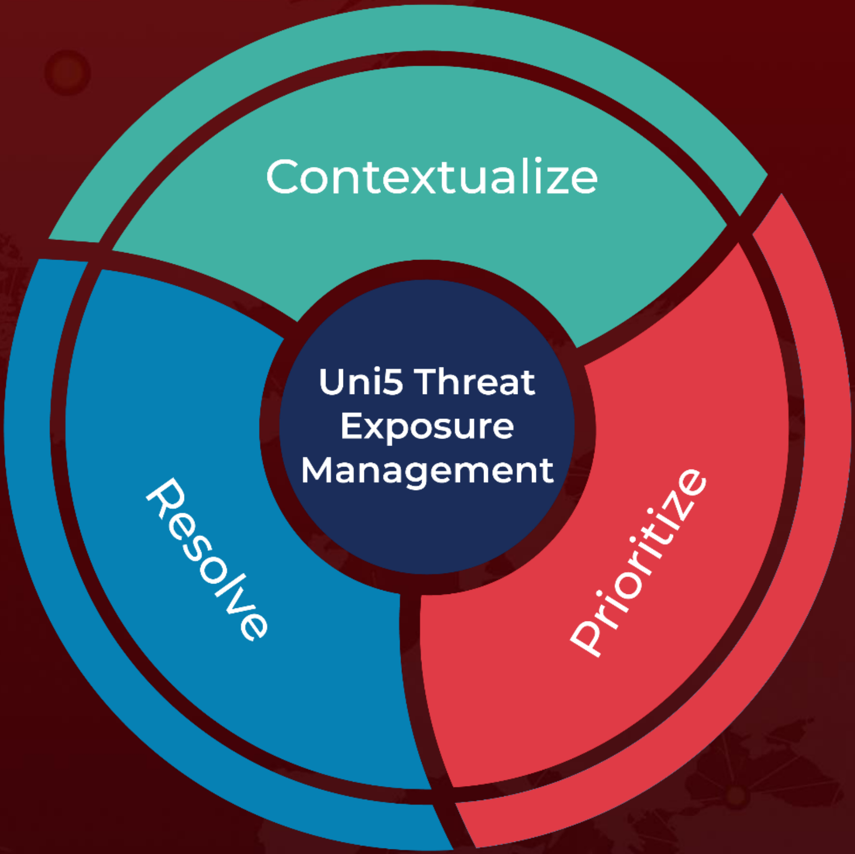
https://www.qnap.com/en/news/2024/official-response-from-qnap-psirt-regarding-recent-security-reports-watchtowr-labs

https://github.com/watchtowrlabs/CVE-2024-27130/blob/main/README.md

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 22, 2024 • 6:00 AM

More at www.hivepro.com