

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## 80K QNAP Devices Vulnerable to Cyberattack

Date of Publication

April 10, 2023

Admiralty Code

A1

TA Number

TA2023176







# Summary

**First Seen:** March 30, 2023

**Affected Products:** QTS, QuTS hero, QuTScloud, QVP (QVR Pro appliances)

**Impact:** Multiple QNAP operating systems have been impacted by two vulnerabilities that could potentially allow remote authenticated users to access secret values.

## CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-27597	QNAP Sensitive Information Disclosure Vulnerability	QTS, QuTS hero, QuTScloud, and QVP OS			
CVE-2022-27598	QNAP Sensitive Information Disclosure Vulnerability	QTS, QuTS hero, QuTScloud, and QVP OS			

## Vulnerability Details

Approximately 80,000 network-attached storage (NAS) appliances running several Quality Network Appliance Provider (QNAP) operating systems (OS) are currently affected by a pair of vulnerabilities, according to reports. Out of the four impacted OS, two remain unpatched. These vulnerabilities, known as CVE-2022-27597 and CVE-2022-27598, are memory access violations that can lead to unstable code and potentially enable an authenticated cybercriminal to execute arbitrary code. The QTS, QuTS hero, QuTScloud, and QVP OS are all affected by these vulnerabilities. Although the QuTScloud and QVP OS are still unpatched, QNAP has announced that it is working urgently to fix the flaws. There have been no reports of these vulnerabilities exploited in the wild.

# Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-27597	QuTScLOUD: All versions, QVP (QVR Pro appliances): All versions, QNAP QTS: before 5.0.1.2346 20230322 & QuTS hero: before h5.0.1.2348 build 20230324	cpe:2.3:a:qnap:qvr:- :*:*:*:*:*:* cpe:2.3:o:qnap:qts:*:*:* :*:*:*:* cpe:2.3:o:qnap:quts_hero:*:*:*:*:*:* o:*:*:*:*:*:* cpe:2.3:o:qnap:qutscLOUD:-:*:*:*:*:*	CWE-125 CWE-489 CWE-1295
CVE-2022-27598	QuTScLOUD: All versions, QVP (QVR Pro appliances): All versions, QNAP QTS: before 5.0.1.2346 20230322 & QuTS hero: before h5.0.1.2348 build 20230324	cpe:2.3:o:qnap:qts:*:*:* :*:*:*:* cpe:2.3:o:qnap:quts_hero:*:*:*:*:* o:*:*:*:*:* cpe:2.3:o:qnap:qutscLOUD:-:*:*:*:*	CWE-125

## Recommendations



To address the vulnerabilities reported in QNAP operating systems, we highly recommend that QNAP users update their operating systems to the latest recommended versions as soon as possible. QNAP has already [resolved](#) the issues in QTS 5.0.1.2346 build 20230322 and later, as well as QuTS hero h5.0.1.2348 build 20230324 and later.



Although the vulnerabilities in QuTS and QVP are still being urgently addressed by QNAP, we advise users to regularly check for updates on this security advisory and update their operating system promptly as soon as the latest recommended version becomes available.



To ensure that your NAS model is up-to-date with the latest updates available, we recommend that you check the [product support status](#) regularly.

If you are using QTS and QuTS hero follow these steps to update your operating system:

1. Log in to QTS and QuTS hero, as an administrator.
2. Go to Control Panel > System > Firmware Update.
3. Under Live Update, click Check for Update.
4. The system will automatically download and install the latest available update.

# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence
<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1543</u></b> Create or Modify System Process
<b><u>T1210</u></b> Exploitation of Remote Services	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1078</u></b> Valid Accounts	<b><u>T1098</u></b> Account Manipulation

## Patch Details

The patch is currently available for QTS and QuTS hero products only.

Patch Link:

<https://www.qnap.com/en/security-advisory/qsa-23-06>

## References

<https://www.qnap.com/en/security-advisory/qsa-23-06>

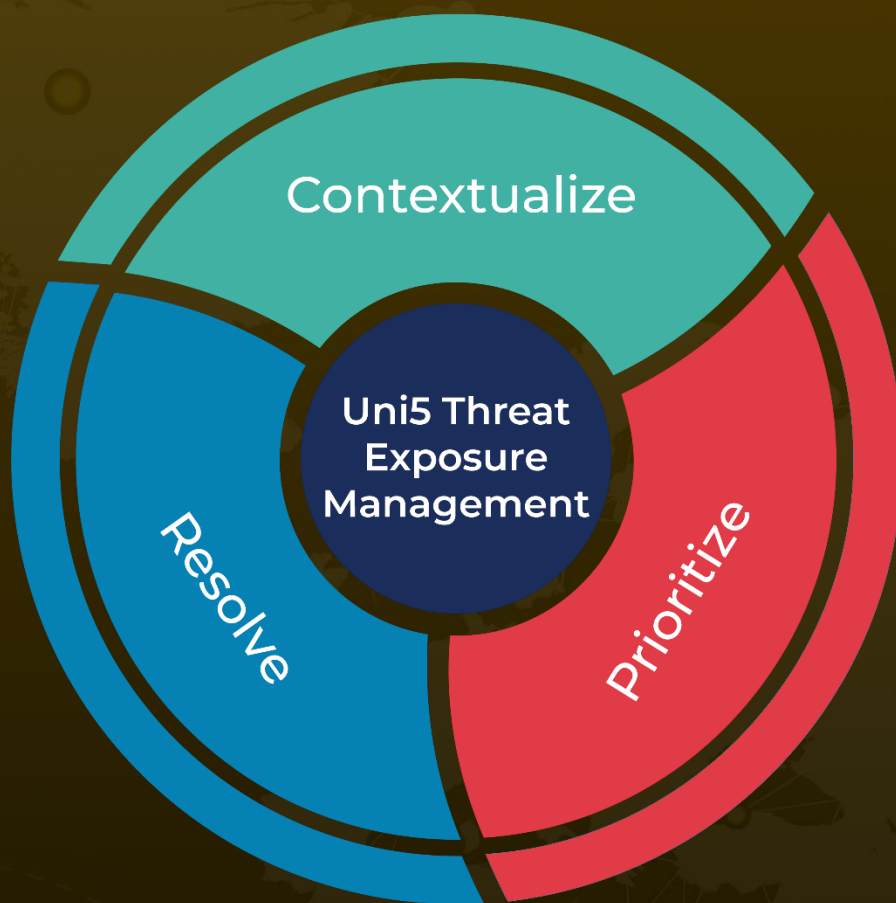
<https://sternumiot.com/iot-blog/qnap-ts-230-nas-vulnerability/>

<https://www.darkreading.com/vulnerabilities-threats/qnap-zero-days-80k-devices-vulnerable-cyberattack>

# 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

**April 10, 2023 • 7:59 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)