Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

QNAP addresses a vulnerability in NAS devices

Date of Publication	Admiralty Code	TA Number
January 31, 2023	A1	TA2023052

Summary

First Seen: January 30, 2023
Affected Products: QNAP QTS and QuTS hero
Impact: Remote attackers can exploit this flaw to inject malicious code.

CVE

CVE	NAME	PATCH
CVE-2022-27596	SQL Injection Vulnerability in QNAP	✓

Vulnerability Details

#1 QNAP has released updates to address a security flaw in its network-attached storage (NAS) devices that allows arbitrary code injection. This vulnerability enables a remote attacker to run any SQL query on the database and has been identified as CVE-2022-27596.

#2 The vulnerability exists as a result of inadequate sanitization of user-supplied data. A remote attacker can execute arbitrary SQL queries within the application database by sending a specially crafted request to the affected device. To install the updates, users are suggested log in as an administrator to QTS or QuTS hero, proceed to Control Panel > System > Firmware Update, and then select "Check for Update" under the "Live Update" section.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-27596	QTS 5.0.1 and QuTS hero h5.0.1	cpe:2.3:a:qnap_systems:qnap_qts:-:*:*:*:*:*:*:* cpe:2.3:a:qnap_systems:qnap_quts:-:*:*:*:*:*:*:*	CWE-89

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0008 Lateral Movement	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1543** Create or Modify System Process
T1210 Exploitation of Remote Services	**T1190** Exploit Public-Facing Application	**T1078** Valid Accounts	**T1098** Account Manipulation

Patch Links

https://www.qnap.com/en/security-advisory/qsa-23-01

References

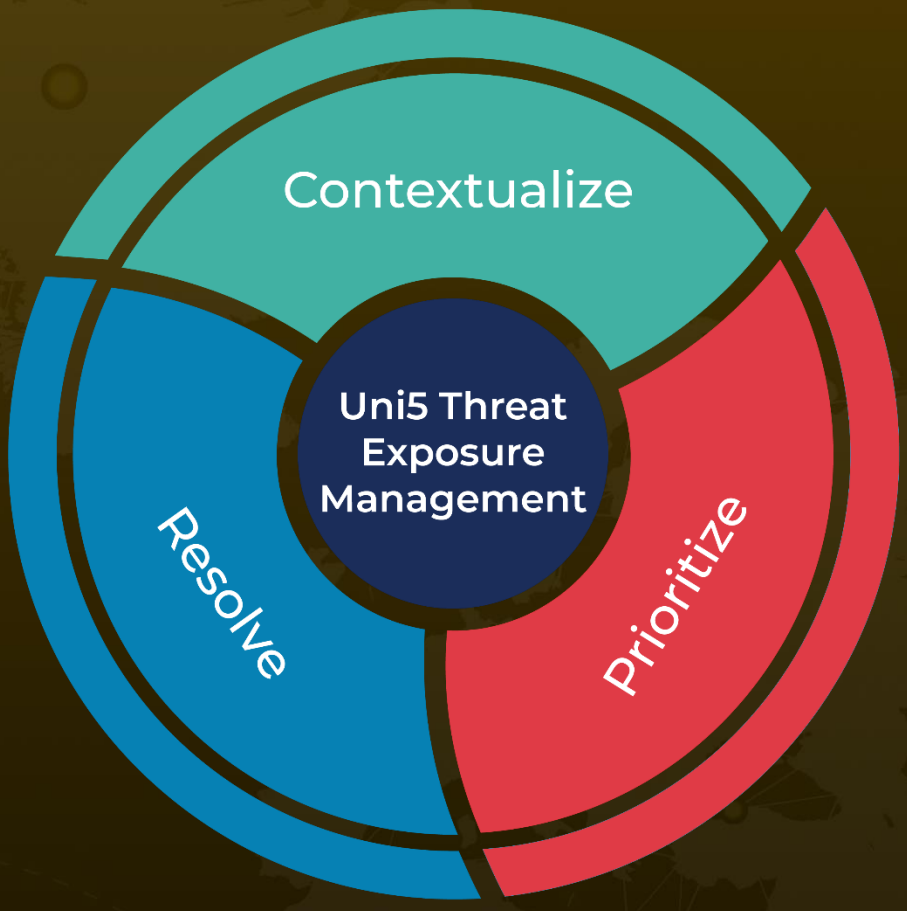
https://www.qnap.com/en/security-advisories?ref=security_advisory_details

https://www.bleepingcomputer.com/news/security/qnap-fixes-critical-bug-letting-hackers-inject-malicious-code/

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

January 31, 2023 . 1:55 AM

More at www.hivepro.com