Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

QNAP Patches Critical Flaw in HBS 3 to Prevent Remote Attacks

Date of Publication	Admiralty Code	TA Number
October 30, 2024	A1	TA2024416

Summary

First Seen: October 29, 2024
Affected Products: QNAP HBS 3 Hybrid Backup Sync
Impact: QNAP has patched a critical vulnerability, tracked as CVE-2024-50388, that was exploited to hack a TS-464 NAS device during the Pwn2Own Ireland 2024 competition. This vulnerability pertains to OS command injection within HBS 3 Hybrid Backup Sync version 25.1.x, which is QNAP's solution for disaster recovery and data backup.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-50388	QNAP HBS 3 Hybrid Backup Sync OS Command Injection Vulnerability	QNAP HBS 3 Hybrid Backup Sync	☒	☒	✓

Vulnerability Details

#1

QNAP has patched a critical vulnerability, tracked as CVE-2024-50388, that was exploited to compromise a NAS device. This OS command injection flaw was discovered in Hybrid Backup Sync (HBS 3), QNAP's unified solution for data backup and disaster recovery, which integrates backup, restoration, and synchronization capabilities across various storage types, including local devices, remote servers, and cloud platforms.

#2

If successfully exploited, CVE-2024-50388 could allow remote attackers to execute arbitrary commands, posing a serious security risk to users' data and systems. To mitigate this threat, QNAP has released an updated version of HBS 3 Hybrid Backup Sync, and users are strongly encouraged to upgrade to the latest release to secure their devices against potential attacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-50388	QNAP HBS 3 Hybrid Backup Sync 25.1.x	cpe:2.3:a:qnap:hbs3_hybrid_backup_sync:*:*:*:*:*:*:*:*	CWE-77

Recommendations

Update: It is recommended to update HBS 3 Hybrid Backup Sync to version 25.1.1.673 or later to mitigate security vulnerabilities. Administrators should log into QTS or QuTS hero, navigate to the App Center, search for "HBS 3 Hybrid Backup Sync," and initiate the update by pressing ENTER and selecting Update.

Restrict Network Access: Limit NAS access to trusted IPs or networks. Avoid exposing NAS devices directly to the internet unless absolutely necessary. Only grant access and administrative privileges to necessary users. Conduct periodic audits to verify and adjust permissions as needed.

Monitor for Unusual Activity: Enable logging and regularly review logs for any unusual access or command execution activities on the NAS device.

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

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1059 Command and Scripting Interpreter	**T1588.005** Exploits		

Patch Details

QNAP has released updates addressing the CVE-2024-50388 vulnerability, and users are strongly advised to upgrade to the patched version, HBS 3 Hybrid Backup Sync 25.1.1.673 or later.

Link: https://www.qnap.com/en-us/security-advisory/qsa-24-41

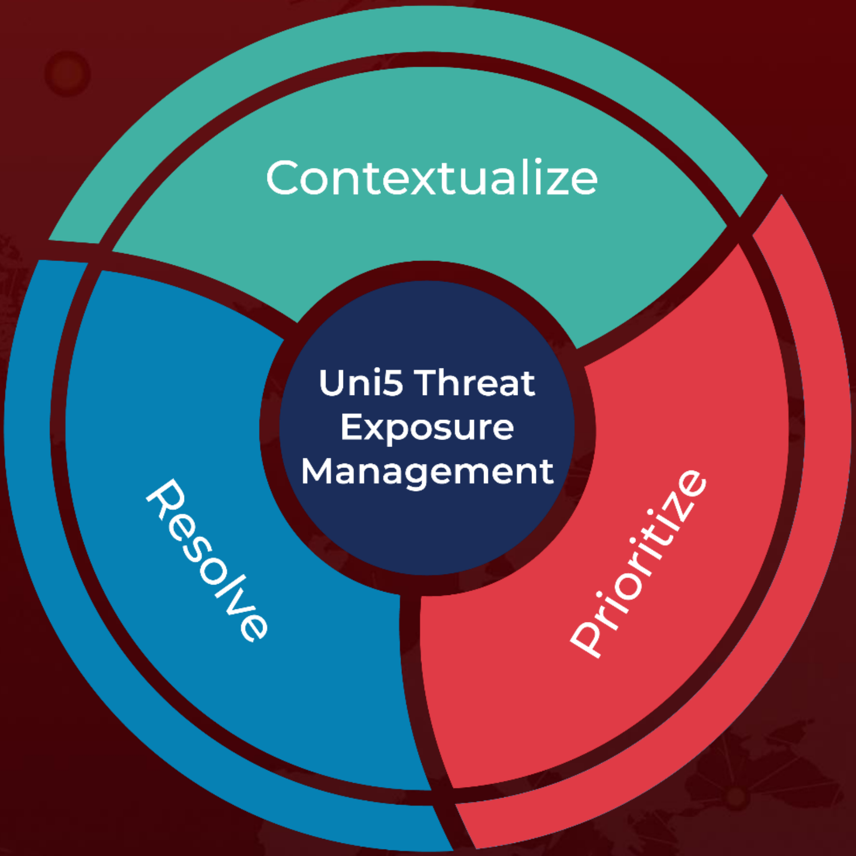
References

https://www.qnap.com/en/security-advisory/qsa-24-41

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

October 30, 2024 • 6:40 PM

More at www.hivepro.com