

Critical QNAP Vulnerability Leads to Code Injection

QNAP Systems this week issued a warning on a critical vulnerability that could allow attackers to inject malicious code on network-attached storage (NAS) devices.

The Taiwan-based manufacturer is known for its NAS appliances and professional network video recorder (NVR) solutions, but also produces various types of networking equipment.

Tracked as CVE-2022-27596 (CVSS score of 9.8), the newly disclosed vulnerability is described as an SQL injection flaw impacting QuTS hero and QTS.

“A vulnerability has been reported to affect QNAP devices running QTS 5.0.1 and QuTS hero h5.0.1. If exploited, this vulnerability allows remote attackers to inject malicious code,” QNAP warns in its advisory.

The company has issued patches for the vulnerability and urges users to update their devices to QTS 5.0.1.2234 build 20221201 and later, or QuTS hero h5.0.1.2248 build 20221215 and later.

“To secure your device, we recommend regularly updating your system to the latest version to benefit from vulnerability fixes,” the manufacturer notes.

Users are advised to update their QNAP appliances as soon as possible, as these devices have long been the target of choice for cybercriminals looking to infect them with ransomware and other malware.

Furthermore, users should ensure that their NAS devices cannot be directly accessed from the internet, and instead secured

behind a firewall or VPN.

Related: QNAP Patches Critical Vulnerability in Network Surveillance Products

Related: QNAP Devices Targeted in New Wave of DeadBolt Ransomware Attacks

Related: QNAP Extends Security Updates for Some EOL Devices

<https://www.securityweek.com/critical-qnap-vulnerability-leads-to-code-injection/>