QNAP fixes critical bugs in QVR video surveillance solution

By
Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)

September 27, 2021 12:56 PM **0**

Network-attached storage (NAS) maker QNAP has patched its QVR video management system against two critical-severity issues that could be exploited to run arbitrary commands.

QNAP promotes its QVR software as a professional solution that allows real-time video monitoring, recording, playback, and alarm notifications when coupled with supported IP cameras.

Total of three security issues

QNAP announced today that it fixed three command injection vulnerabilities in the QVR software for managing video surveillance, two of them receiving a critical severity score of 9.8 out of 10.

Tracked as CVE-2021-34351 (https://nvd.nist.gov/vuln/detail/CVE-2021-34351) and CVE-2021-34348 (https://nvd.nist.gov/vuln/detail/CVE-2021-34348), the pair of critical bugs could allow a remote attacker to run commands on vulnerable systems that could lead to taking full control of the device.

Apart from these two security issues, QNAP fixed another one tracked as CVE-2021-34349 (https://nvd.nist.gov/vuln/detail/CVE-2021-34349). It is from the same class but with a lower severity score, 7.2 out of 10.

The difference in severity is due to the privileges required to exploit the bugs: none are needed for the critical ones, while an attacker leveraging the high-severity issue needs high privileges.

QNAP notes that the two critical vulnerabilities affect certain products running QVR that have reached end of life (EoL). Even if the devices are no longer supported, many customers are likely still using them, prompting the company to release a software update (QVR 5.1.5 build 20210803).

> “Two command injection vulnerabilities have been reported to affect certain QNAP EOL devices running QVR. If exploited, these vulnerabilities allow remote attackers to run arbitrary commands” - QNAP (https://www.qnap.com/en/security-advisory/QSA-21-35)

It is unclear if any of the bugs are being exploited been exploited. BleepingComputer has reached out to QNAP for clarification about this and is currently awaiting a reply.

Attractive devices

Provided that the devices are used for video surveillance by businesses of various sizes (enterprise, SMB, SOHO), threat actors may be incentivized to exploit these vulnerabilities.

Earlier this year, in a campaign from what became known as Qlocker ransomware, a cybercriminal gang leveraged a vulnerability (hardcoded credentials (https://www.bleepingcomputer.com/news/security/qnap-removes-backdoor-account-in-nas-backup-disaster-recovery-app/)) in QNAP NAS devices to encrypt files using the 7-Zip archive utility.

Victims, mostly consumers and small-to-medium business owners, were asked just $500 for file recovery, a very small price that many were willing to pay.

It is estimated that the actors behind Qlocker ransomware made at least $260,000 in just five days (https://www.bleepingcomputer.com/news/security/a-ransomware-gang-made-260-000-in-5-days-using-the-7zip-utility/) in ransoms collected from their victims.

Back in March, hackers leaked footage after gaining access to live surveillance cameras managed by Verkada and widely used across the U.S. by big-name companies (Tesla, Equinox), healthcare clinics, prisons, and banks.

Related Articles:

New Windows security updates break network printing (https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/)

QNAP works on patches for OpenSSL bugs impacting its NAS devices (https://www.bleepingcomputer.com/news/security/qnap-works-on-patches-for-openssl-bugs-impacting-its-nas-devices/)

Fortinet delays patching zero-day allowing remote server takeover (https://www.bleepingcomputer.com/news/security/fortinet-delays-patching-zero-day-allowing-remote-server-takeover/)

The Week in Ransomware - September 24th 2021 - Targeting crypto (https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-24th-2021-targeting-crypto/)

Emergency Google Chrome update fixes zero-day exploited in the wild (https://www.bleepingcomputer.com/news/security/emergency-google-chrome-update-fixes-zero-day-exploited-in-the-wild/)