Critical Vulnerability in Hikvision Storage Solutions Exposes Video Security Data

Video surveillance giant Hikvision this week informed customers that it has patched a critical vulnerability affecting its Hybrid SAN and cluster storage products.

The vulnerability, tracked as CVE-2023-28808, has been described by the vendor as an access control issue that can be exploited to obtain administrator permissions by sending specially crafted messages to the targeted device.

The impacted products are used by organizations to store video security data, and an attacker exploiting the vulnerability could gain access to that data.

In a notification sent by Hikvision to partners – a copy was also shared with *SecurityWeek* – the company said it's not aware of in-the-wild exploitation.

"While Hikvision is not aware of this vulnerability being exploited in the field, we recognize that some of our partners may have installed Hikvision equipment that is affected by this vulnerability and we strongly encourage them to work with their customers to install the patch and ensure proper cyber hygiene," the company told partners.

Hikvision noted in its advisory that an attacker needs to have network access to the targeted device in order to exploit CVE-2023-28808.

However, Arko Dhar, the CTO of Redinent, the India-based CCTV and IoT cybersecurity company credited for finding the

vulnerability, told *SecurityWeek* that many impacted systems are exposed to the internet and remote exploitation is possible.

“The Hybrid SAN storage is primarily meant to store CCTV video recordings. But it can also be configured to store business data as well. The impact is very wide – an attacker can delete video recordings and business data at the same time, delete backups and cause significant impact to the business,” Dhar warned.

Redinent’s researchers discovered the vulnerability in late December 2022 and the flaw was reported to the vendor through CERT India in January.

Hikvision announced on April 10 that patches are included in version 2.3.8-8 for Hybrid SAN and version 1.1.4 for cluster storage devices. The vendor has provided detailed instructions for installing the updates.

Related: Vulnerability Allows Hackers to Remotely Tamper With Dahua Security Cameras

Related: Critical Vulnerability in Hikvision Wireless Bridges Allows CCTV Hacking

Related: QNAP Patches Critical Vulnerability in Network Surveillance Products

https://www.securityweek.com/critical-vulnerability-in-hikvision-storage-solutions-exposes-video-security-data/