500 Frank W Burr Blvd.
Teaneck, NJ 07666
https://HanwhaVisionAmerica.com

12/13/2023

WAVE Sync Vulnerability Report (CVE-2023-6263)

■ OVERVIEW

- A vulnerability has been discovered in the WAVE Sync cloud authentication mechanism which could allow an attacker to gain access to a WAVE system.
- The vulnerability exploited a Man-In-The-Middle attack allowing an attacker to spoof a legitimate connection to gain access to the system.

■ SOLUTION AND REQUIRED ACTION

- **The vulnerability has been remediated on the WAVE Sync backend on September 22th, 2023.** Once the vulnerability was discovered and reported, the issue was investigated and remediated within 1 week.
- Immediate Action: We strongly urge you to change the VMS server owner's (user "admin") local password.
- Perform users and permissions review. The audit trail can be utilized to user activities.

■ AFFECTED SOFTWARE

All WAVE systems connected to WAVE Sync were affected. Systems not connected to WAVE Sync are not vulnerable.

- **During our investigation, we have not found any evidence of this vulnerability being exploited yet. Vulnerability exploitation is relatively hard and demands multiple prerequisites, yet still we recommend performing certain actions.**

500 Frank W Burr Blvd.
Teaneck, NJ 07666
https://HanwhaVisionAmerica.com

■ RISK ANALYSIS

Review Opinion	Severity
The vulnerability requires an attacker with a high level of skill to develop custom code, connect perform a man-in-the-middle attack, and then wait for an authorized user to connect. Once this connection is made, the authorization headers are obtained and replayed, allowing an attacker access to the system. Systems which are not connected to the WAVE Sync cloud are not affected.	High

■ FUTURE MEASURES:

- We are constantly enhancing our security protocols and will continue to conduct regular security audits to prevent such incidents in the future. We also plan to expand our collaboration with third-party security experts to ensure our systems remain resilient against evolving cyber threats.

If you have any questions, please feel free to reach out the Hanwha S-CERT team at secure.cctv@hanwha.com or your local Technical Support Team.