Arteco Security Advisory

Camera Driver Buffer-Overflow Vulnerability

Date Published: 9 October 2024.

Affected Vendor/Product: Omnia VMS (selected camera drivers)

Status for Arteco Products: *Not applicable to Arteco-native products* (no direct impact).

Summary

A buffer overflow vulnerability exists in certain camera drivers included with OMNIA VMS Server Suite. Under strict conditions, an attacker with access to the internal network could exploit this vulnerability to execute commands on the Server.

Products/Versions Affected

Selected camera drivers within the OMNIA VMS Server Suite 24.3, versions prior to the patched release.

Issue

A buffer overflow allows an attacker to potentially execute arbitrary code on the Recording Server with the user permissions of that server.

Recommended Mitigations

- Apply the latest Omnia VMS Server Suite update from Arteco that fixes the vulnerability.
- Restrict network access: Ensure that only trusted, authorized devices can connect to the internal network segment where the OMNIA VMS Server resides.
- Minimize privileged access: Limit users and services with rights on the OMNIA VMS Server; apply least-privilege principles.
- Monitor server logs and alert for anomalous execution or unexpected driver behavior.
- Segment and isolate camera networks: Place cameras and associated drivers in segregated network zones to prevent lateral movement.
- Consider rotating credentials and reviewing driver configurations if you suspect exposure or outdated versions.