CISA flags critical flaws in EseeCloud IP camera app and firmware



CISA published an ICS advisory on three vulnerabilities in EseeCloud App and firmware that could let an attacker take control of IP cameras. The CVSS v3 score is 9.8.

- Affected: EseeCloud App up to 4.9.6 and EseeCloud Firmware up to 4.9.86.0.
- Three CVEs: CVE-2026-107617, CVE-2026-97858 and CVE-2026-105664.
- Weakness types: hard-coded credentials, improperly controlled modification of object attributes, and observable response discrepancy.
- One flaw lets an attacker log in to devices using a hard-coded credential.
- The vendor, Guangzhou Juan IoT Technology, did not respond to CISA's coordination attempts.

CISA has released an industrial control systems advisory covering Guangzhou Juan IoT Technology's EseeCloud products. Successful exploitation of the three listed vulnerabilities could allow an attacker to gain control over affected IP cameras. The advisory gives a CVSS v3 score of 9.8.

What is affected

The advisory lists EseeCloud App versions up to and including 4.9.6, and EseeCloud Firmware versions up to and including 4.9.86.0. Each of the three CVEs applies to both: CVE-2026-107617, CVE-2026-97858 and CVE-2026-105664.

The weaknesses are use of hard-coded credentials, improperly controlled modification of dynamically-determined object attributes, and observable response discrepancy. For CVE-2026-107617, an attacker can use a hard-coded credential to log in to EseeCloud devices.

Vendor status and context

According to CISA, the vendor did not respond to its coordination attempts. The excerpt we reviewed does not describe a vendor fix. Organisations should therefore plan around compensating controls rather than wait for a patch.

CISA lists the affected sectors as Energy, Communications, Transportation Systems, Financial Services and Government Services and Facilities, with deployment worldwide. The company is headquartered in China.

What to do

First establish whether any EseeCloud-based cameras are in use, including in branches, facilities and third-party managed sites. Then limit their network exposure while the vendor position remains unclear.

What to do now

1. Inventory all IP cameras and apps using EseeCloud, including those run by third parties.
2. Check whether affected versions (App up to 4.9.6, firmware up to 4.9.86.0) are deployed.
3. Remove these cameras from direct internet exposure and isolate them in a segmented network.
4. Restrict access to camera management interfaces to authorised administrators only.
5. Monitor for unexpected logins or configuration changes on these devices.
6. Ask suppliers for the vendor's remediation status, and consider replacing devices if no fix is offered.