CISA flags missing authentication in Swann SWIFI-SE2KIC cameras



CISA published an advisory on Swann SWIFI-SE2KIC cameras running firmware 2.0.22 or earlier. A missing-authentication flaw lets someone on the local network view live video without logging in. CVSS v3 is 6.2.

- Affected: SWIFI-SE2KIC firmware 2.0.22 and earlier.
- Three CVEs are listed: CVE-2026-107605, CVE-2026-107606 and CVE-2026-107607.
- The weakness is Missing Authentication for Critical Function.
- An attacker on the local network could view live video without authentication.
- CVSS v3 score is 6.2; Swann has issued interim mitigations.

CISA has published an industrial control systems advisory covering the Swann Communications SWIFI-SE2KIC camera. The product is listed under the Commercial Facilities sector, is deployed worldwide, and the vendor is headquartered in Australia.

What the advisory says

Firmware versions 2.0.22 and earlier are affected by three vulnerabilities: CVE-2026-107605, CVE-2026-107606 and CVE-2026-107607. The weakness is classed as **Missing Authentication for Critical Function**. According to the advisory, an attacker on the local network could view the live video feed without authenticating. The CVSS v3 score is 6.2.

Mitigation

Swann Communications has provided interim security measures, including keeping the camera behind a secured network. The advisory directs readers to the vendor's support channel for further details. The source excerpt does not mention a fixed firmware version, so organisations should confirm the current status with the vendor.

The exposure requires local network access, so the practical risk depends on how well camera networks are segmented from user and guest networks. Organisations that use these cameras in offices, branches or retail spaces should first establish whether any are deployed, then check firmware versions and network placement.

What to do now

1. Check asset inventories and physical-security records for SWIFI-SE2KIC cameras and note their firmware versions.
2. Place any affected cameras on an isolated network segment, separate from corporate, guest and user networks.
3. Apply Swann's interim measures and contact Swann support to confirm whether a fixed firmware is available.
4. Restrict who can reach camera networks, and review whether live feeds could expose sensitive areas or people.
5. Record the exposure and the decisions taken under your risk-management process.