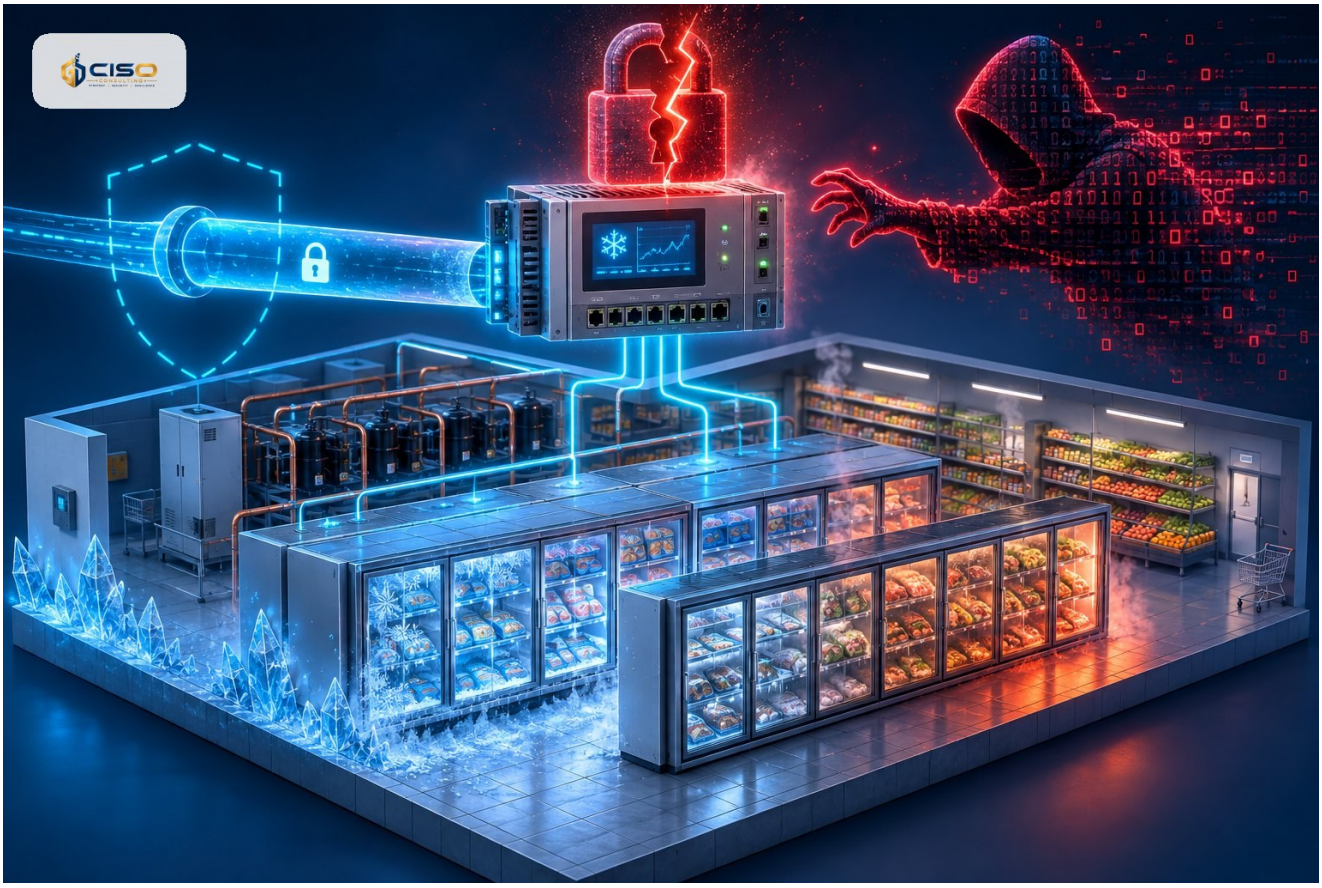
CISA flags critical unpatched flaw in Danfoss AK-SM 8xxA refrigeration controllers



CISA warns that CVE-2026-129713 (CVSS 9.8) in Danfoss AK-SM 8xxA controllers allows unauthenticated attacks and possible remote code execution. No patch exists yet; isolation and VPN-only access are advised.

- CVE-2026-129713 is a stack-based buffer overflow in the server of Danfoss AK-SM 8xxA controllers, scored 9.8.
- An unauthenticated attacker can restart the server and potentially run code with the web server's privileges.
- Danfoss plans a fix in software version 5.5.x; no patch is available yet.
- The product line manages refrigeration, and on some models lighting and HVAC, in food retail.
- Danfoss controllers were recently hit in attacks on European supermarkets that shut down or

> altered cooling.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned of a critical vulnerability in Danfoss AK-SM 8xxA Series controllers, which food retailers use to manage commercial refrigeration and, depending on the model, lighting and HVAC.

The vulnerability

The flaw is tracked as **CVE-2026-129713** and carries a severity score of 9.8. It is a stack-based buffer overflow in the controller's server. According to CISA, an attacker needs no authentication to trigger it, can cause the server to restart, and may achieve remote code execution with the privileges of the web server. The affected line is the AK-SM 800A Series, including the 820A, 850A and 880A models. CISA notes the devices are deployed worldwide, though the number is unclear.

Status and context

On November 20, Danfoss published an advisory stating that the issue will be addressed in the upcoming software version 5.5.x, which will also remove the option to disable 'Strict mode'. No patch is available at present.

The warning follows recent incidents in Europe in which Danfoss and other refrigeration controllers at supermarkets were compromised and cooling was shut down or settings altered. Reporting also describes a case affecting cold storage at a French blood service supplier.

Interim measures

Until a fix is released, CISA advises keeping controllers off the public internet, minimizing network exposure, separating control systems from business networks behind firewalls, and using up-to-date VPNs where remote access is required.

What to do now

1. Inventory Danfoss AK-SM 8xxA controllers (820A, 850A, 880A) across stores, warehouses and cold-chain sites, including those run by third-party facility providers.
2. Confirm none are reachable from the public internet and remove any direct exposure.
3. Segregate these controllers from business networks behind firewalls, in line with NCA OTCC expectations for operational technology.
4. Restrict remote access to up-to-date VPNs and review recent access logs for unexpected restarts or setting changes.
5. Track the Danfoss advisory and plan to deploy version 5.5.x once released, with a rollback and testing plan.

6. Ask refrigeration and facility suppliers to confirm their exposure and interim controls in writing.