# Danfoss AK-SM 8xxA controllers: unauthenticated buffer overflow flagged by CISA



CISA reports CVE-2026-129713, a critical flaw (CVSS v3 9.8) in Danfoss AK-SM 8xxA controllers up to version 5.4.0. A fix is planned in release 5.5.x.

- CVE-2026-129713 is a stack-based buffer overflow in an unauthenticated CGI handler.
- Affected: Danfoss AK-SM8xxA version 5.4.0 and earlier; CVSS v3 score 9.8.
- Crafted HTTP/S POST requests can corrupt memory and restart the webserver, with potential code execution at webserver privileges.
- No authentication is needed to exploit it.
- Danfoss plans a fix in software release 5.5.x and will remove the option to disable Strict Mode in future releases.

## What was reported

CISA has published an industrial control systems advisory covering the Danfoss AK-SM 8xxA Series, a controller used in commercial facilities. The flaw, tracked as CVE-2026-129713, is a stack-based buffer overflow in a CGI handler that does not require authentication. It carries a CVSS v3 score of 9.8.

An attacker who can reach the device could send specially crafted HTTP/S POST requests. The advisory describes memory corruption and a webserver restart, with arbitrary code execution at webserver privileges as a potential outcome. Versions up to and including 5.4.0 are listed as affected.

## Vendor response

Danfoss states the issue will be addressed in an upcoming AK-SM 800A Series software release, version 5.5.x. It also intends to remove, in future releases, the ability for users to disable Strict Mode. The source does not mention a fix available today or reports of active exploitation.

## What this means for operators

Organisations running these controllers in commercial buildings, such as retail, food storage or facilities management, should treat the exposure as serious because no credentials are needed. Until a patched release is available, reducing network reachability of the web interface is the most practical step.

- Identify any AK-SM 8xxA units and their software versions.
- Confirm they are not reachable from the internet or untrusted networks.
- Track Danfoss announcements for release 5.5.x.

## What to do now

1. Inventory all Danfoss AK-SM 8xxA controllers and record their software versions.
2. Verify none are exposed to the internet; restrict web access to trusted management networks.
3. Place the controllers behind segmentation and firewall rules that limit HTTP/S access to approved hosts.
4. Monitor for unexpected webserver restarts or unusual POST traffic to these devices.
5. Plan the upgrade to release 5.5.x once Danfoss publishes it, and track the vendor's notices.