contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Danfoss AK-SC 355: new CVE

CVE-2026-127057 · record published 20 November 2026

Analysis Report

All versions of the Danfoss AK-SC 355 and AK-SM 800 Series are affected and the vendor's record names no fixed release. Operators of these devices should remove any public IP exposure immediately and …

PREPARED BY	NamiQ	DATE	21 November 2026
FACTS AS OF	21 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 9.9**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/danfoss-ak-sc-355-cve-2026-127057

The bottom line

> *All versions of the Danfoss AK-SC 355 and AK-SM 800 Series are affected and the vendor's record names no fixed release. Operators of these devices should remove any public IP exposure immediately and change credentials before planning migration to the AK-SM800A series.*

At a glance

Fact	Detail
Product	Danfoss AK-SC 355 (CVE-2026-127057)
Severity	Critical: 9.9 (CVSS 4.0)
Status	A new CVE record, published by Danfoss on 20 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 21 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No fixed release. The record lists all versions as affected and names no unaffected release. The vendor says to migrate to the AK-SM800A series for ongoing security updates.
Who looks first	Operators of a Danfoss AK-SC 355 or AK-SM 800 Series controller, particularly where the device is reachable from the internet or from an untrusted network segment. The record names both product lines.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Danfoss AK-SC 355 or AK-SM 800 Series controller?	Nothing to do for this CVE.	Check whether it is reachable from outside your site network.
Is the device reachable from the internet or an untrusted network?	Lower risk; still check that default credentials have been changed.	Remove the public IP exposure immediately, then check credentials.
Have the default credentials been changed on this unit?	Change them now; the default credentials are documented in the product manual.	Still plan migration to the AK-SM800A series; no patch exists for this product line.

What it is

An attacker who can reach the device over a network can authenticate using credentials the vendor published in the product manual. No vulnerability in the software itself is needed; the credentials are simply known, documented, and unchanged on delivery.

Why it matters

CWE-1392 means the credentials needed to log in were printed in the product manual at manufacture. Anyone with the manual can try them without technical skill. The record scores this 9.9 on CVSS 4.0. No patch exists; the vendor's record recommends replacing the unit with the current-generation AK-SM800A series. Our reading is that units facing the internet are at the greatest risk, but a local-network attacker can reach this just as easily once inside a building network.

Things people will get wrong

- Changing the password fully resolves this. The record also names 'known passwords' as a risk alongside default ones. No patch exists; the vendor recommends migrating to the AK-SM800A series rather than patching the current product line.
- Only the AK-SC 355 is affected. The record description names both the AK-SC 355 and the AK-SM 800 Series as vulnerable to this flaw.

How we would triage it

This is our judgement.

Step 1: Find which Danfoss AK-SC 355 or AK-SM 800 units you run

- Check your building management or refrigeration control inventory for Danfoss AK-SC 355 or AK-SM 800 Series devices.
- Confirm whether any unit has a public IP address or is reachable from outside your site network; the vendor's record identifies this as the primary risk factor.

Step 2: Remove or restrict network exposure

- If the unit has a public IP address, the vendor's record says to install it without public IP exposure; place it behind a firewall or VPN immediately.
- Block the device's management interface from any untrusted network segment until credentials are verified and migration is planned.

Step 3: Change credentials on every affected unit

- Log in to each unit and replace the default credentials with a unique password not found in any product manual.
- The record identifies CWE-1392: default credentials are documented in the manual; changing them removes the most accessible attack path.

Step 4: Plan migration to the AK-SM800A series

- The vendor's record says to update the fleet to the AK-SM800A series to receive ongoing cybersecurity updates; no patch is listed for the current product line.
- The record names no unaffected release for the AK-SC 355 or AK-SM 800 Series; replacement is the only remediation path the vendor states.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been made aware of CVE-2026-127057, which affects all versions of the Danfoss AK-SC 355 and AK-SM 800 Series controllers. No patch is available; the vendor's record says all versions are affected and recommends migrating to the AK-SM800A series. The flaw allows anyone with the product manual to authenticate using documented default credentials. Could you confirm: whether we run any of these units, whether any are reachable from outside our network, and whether default credentials have been changed. Please provide written confirmation of the current status and your planned remediation steps.*

The weakness behind it

The record classes this as CWE-1392.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record

says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	The record says authentication with documented default credentials is the attack path; using known, pre-set credentials to gain access would typically be classed as valid account use.
External Remote Services (T1133): Using a remote-access service such as a VPN or remote desktop to get into the network.	Initial Access: getting in	The vendor's record identifies public IP exposure as a risk factor; an internet-facing unit accessed with default credentials would likely align with external remote service exploitation.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *The Danfoss legacy AK-SC 355 and AK-SM 800 Series are vulnerable to unauthorized access when default credentials or known passwords are used for authentication. These products were manufactured with default credentials documented in the product manual. All versions are affected.*

Versions of Danfoss AK-SC 355 the record lists as affected:

- all versions up to and including latest

The record gives no version ranges. Use the vendor's advisory for the affected versions.

What the record says to do about it, in the vendor's words:

> ** Install according to the instructions of the manual, avoiding public IP exposure • Update the fleet (AK-SC355, AK-SM800) to current generation products (AK-SM800A series), to ensure receiving continuous cybersecurity updates.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs

nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-127057
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-127057
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- Whether the flaw can be exploited without the product manual, for example by credential reuse or brute force, or only via the documented defaults the record names.
- Whether the AK-SM800A series the vendor recommends as a replacement is itself affected by this or related weaknesses.
- Whether a firmware update path exists for current units, or whether hardware replacement is the only remediation the vendor offers.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 21 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping",

"How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-127057: score 9.9, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	Low	Some data exposed.
Subsequent systems: integrity	Low	Some data or behaviour can be altered.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
20 November 2026	CVE record published by Danfoss.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
AK-SC 355 or AK-SM 800 facing the internet with default credentials in place	Medium	Now

AK-SC 355 or AK-SM 800 facing the internet, credentials changed from defaults	Low	This week
AK-SC 355 or AK-SM 800 on internal network only, default credentials unchanged	Low	This week
AK-SC 355 or AK-SM 800 on internal network only, credentials changed from default	None	None for this CVE
Unit already replaced with the AK-SM800A series	None	None for this CVE

Appendix 4. Definition of done

- Every Danfoss AK-SC 355 you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-127057: https://www.cve.org/CVERecord?id=CVE-2026-127057
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: www.danfoss.com: https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2026-12-02/