contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Danfoss AK-SM 800A Series exploited

CVE-2025-41450 · on CISA's exploited list since 25 November 2026

Analysis Report

Anyone running a Danfoss AK-SM 8xxA Series controller on firmware before version 4.2 must update by 9 December 2026. Check the installed firmware version on each device first.

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.2**	STATUS	On CISA's exploited list; due 9 December 2026

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-sm-800a-series-cve-2025-41450

The bottom line

> *Anyone running a Danfoss AK-SM 8xxA Series controller on firmware before version 4.2 must update by 9 December 2026. Check the installed firmware version on each device first.*

At a glance

Fact	Detail
Product	Danfoss AK-SM 800A Series (CVE-2025-41450)
Severity	High: 8.2 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 9 December 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 26 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Firmware version 4.2. The CVE record states all versions prior to 4.2 are affected; 4.2 is the first version the record identifies as outside the affected range.
Who looks first	Operators running Danfoss AK-SM 8xxA Series controllers on any firmware version before 4.2. The risk is higher where the device's web interface is reachable from an untrusted network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Danfoss AK-SM 8xxA Series controller?	Nothing to do for this CVE.	Check the installed firmware version.
Is the installed firmware version earlier than 4.2?	No action needed for this CVE; monitor for future advisories.	Plan an update to version 4.2 or later.
Can the device's web interface be reached from outside your site network?	Still update within CISA's window; restrict access while arranging it.	Treat this as urgent — restrict access and update before the deadline.

What it is

An attacker who can reach the device's web interface can generate a report without authenticating. The record says the report reveals internal IP addresses, usernames, and store names associated with the device.

Why it matters

The weakness is an authentication bypass, not a weakened check: CWE-305 means the authentication step for a specific web function can be skipped entirely. The data exposed — internal IP addresses, usernames, and store names — is reconnaissance material that maps the network and names accounts for further attempts. Our reading is that this makes the flaw useful as an early step in a broader intrusion, not only a one-off information grab. The EPSS score of 0.00513 reflects limited observed exploitation to date, not limited usefulness to an attacker who can reach the interface.

Things people will get wrong

- This only matters if the controller faces the internet. The record does not restrict the flaw to internet-facing devices. Any attacker who can reach the web interface on any network segment can generate the report without authenticating.
- Authentication is just weakened, not absent. The record lists CWE-305 — authentication bypass by primary weakness — which means authentication for this function can be skipped entirely, not merely made easier to pass.

How we would triage it

This is our judgement.

Step 1: Confirm the firmware version on each device

- Locate the AK-SM 8xxA Series administration interface and note the current firmware version; the record states all versions before 4.2 are affected.
- Record the version for each unit in service so nothing is missed.

Step 2: Restrict access to the web interface

- While arranging the update, limit network access to the device's web interface to known management addresses only.
- No vendor advisory was available for review, so access restriction is a temporary measure, not a substitute for updating.

Step 3: Apply the firmware update to version 4.2

- The record names version 4.2 as the first version outside the affected range; update each device to 4.2 or later.
- Follow the update procedure in the device documentation; no vendor advisory text was available to supplement it.

Step 4: Check for signs of access if a device was exposed

- Review device access logs for unexpected requests to the web report function, particularly from addresses not used for management.
- If unfamiliar source addresses appear, treat internal IP addresses and usernames from the report as potentially known to an attacker and review account access accordingly.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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 run Danfoss AK-SM 8xxA Series controllers and have learned of CVE-2025-41450, a confirmed vulnerability in all firmware versions before 4.2. It allows an unauthenticated attacker who can reach the web interface to generate a report that exposes internal IP addresses, usernames, and store names. CISA has set a remediation deadline of 9 December 2026. Please confirm: (1) whether and where we run this device; (2) the firmware version on each unit; (3) whether the web interface is reachable from outside our site network; and (4) when we can update to version 4.2. We need written confirmation of the installed version and update status by 9 December 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected HTTP requests to the web report endpoint in device access logs, particularly from addresses not recognised as management hosts.
- Access to the device web interface from unusual source addresses or outside normal maintenance windows.

The weakness behind it

The record classes this as CWE-305 (Authentication Bypass by Primary Weakness).

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
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a web interface; an attacker with network access would likely send a crafted request to bypass the authentication check and trigger report generation, fitting an exploit of a public-facing application.
System Information Discovery (T1082): Reading the details of a system, such as its version and configuration.	Discovery: looking around	The report exposes internal IP addresses and usernames — network and system information that would typically be gathered in a discovery phase before moving further into the environment.
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	Usernames obtained from the report could be used in subsequent valid-account attempts against this or related systems on the same network.

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

CISA's catalogue entry:

> *Danfoss AK-SM 800A Series contains an improper authentication vulnerability that could allow an attacker to generate a web report exposing sensitive information, including internal IP addresses, usernames, and store names.*

The CVE record, published by Danfoss on 8 May 2025:

> *Improper Authentication vulnerability in Danfoss AKSM8xxA Series.This issue affects Danfoss AK-SM 8xxA Series prior to version 4.2*

Versions of Danfoss AK-SM 8xxA Series the record lists as affected:

- all versions before 4.2

The affected ranges end before 4.2. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

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-2025-41450
```

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-2025-41450
```

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 a temporary workaround exists — CISA directs operators to follow vendor instructions, but no vendor advisory page was available for review.
- The exact release date of firmware version 4.2.
- Whether the flaw requires the web interface to be network-reachable, or whether local access to the device is sufficient to trigger it.
- Whether the CISA product name 'AK-SM 800A Series' and the CVE record name 'AK-SM 8xxA Series' cover exactly the same set of models.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 26 November 2026; the vendor's advisory wins where it differs.
- 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-2025-41450: score 8.2, `CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	High	Needs conditions outside the attacker's control.
Privileges required	None	No account is needed.
User interaction	Required	A person must click, visit or open something.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	Low	Some data or behaviour can be altered.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
8 May 2025	CVE record published by Danfoss.
25 November 2026	CISA added it to its list of exploited vulnerabilities.
9 December 2026	CISA's deadline for US federal agencies.

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
Device web interface reachable from an untrusted or external network, firmware before 4.2	High	Before 9 December 2026, sooner if possible
Firmware version not yet confirmed and device is in service	Medium	This week
Device on a site network only, no external access, firmware before 4.2	Medium	Before 9 December 2026

Device confirmed on firmware 4.2 or later	None	None for this CVE

Appendix 4. Definition of done

- Every Danfoss AK-SM 800A Series you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2025-41450: https://www.cve.org/CVERecord?id=CVE-2025-41450
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: www.danfoss.com: https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/dsa-2025-03-01/