contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Danfoss AK-SM 800A Series exploited

CVE-2023-25915 · on CISA's exploited list since 25 November 2026

Analysis Report

Any organisation running a Danfoss AK-SM800A on firmware before 3.3 must act before 28 November 2026. Find the firmware version on each unit today; if it is below 3.3, restrict who can log in while …

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	STATUS	On CISA's exploited list; due 28 November 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-2023-25915

The bottom line

> *Any organisation running a Danfoss AK-SM800A on firmware before 3.3 must act before 28 November 2026. Find the firmware version on each unit today; if it is below 3.3, restrict who can log in while you arrange an update.*

At a glance

Fact	Detail
Product	Danfoss AK-SM 800A Series (CVE-2023-25915)
Severity	Critical: 9.9 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 28 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 25 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The CVE record lists AK-SM800A versions before 3.3 as affected; 3.3 is the implied boundary. No vendor advisory was readable to confirm it as the fixed release.
Who looks first	Operators of a Danfoss AK-SM800A controller on firmware before version 3.3, particularly where the management interface is reachable from more than one user across a network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you operate a Danfoss AK-SM 800A Series (AK-SM800A) controller?	Nothing to do for this CVE.	Check the firmware version on each unit (next question).
Is any unit running firmware below version 3.3?	The record does not list your version as affected; monitor for further guidance.	Restrict login access now and arrange the firmware update.
Can anyone other than a trusted administrator log in to the device remotely?	Lower immediate risk; still apply the firmware update before 28 November 2026.	Restrict login access immediately; treat this as high priority.

What it is

A logged-in remote user can pass malformed input that the device does not validate correctly, allowing them to run arbitrary commands on the AK-SM800A.

Things people will get wrong

- A login requirement means only an insider can exploit this; external attackers cannot reach it. The record says the attacker is remote and authenticated. A credential obtained through any means — reuse, sharing — is enough to reach the flaw from outside the site.
- A score of 9.9 means no authentication is needed. The record and the condition notes both state the attacker must be logged in. The high score reflects the severity of arbitrary command execution once inside, not ease of initial access.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on each AK-SM800A

- Log in to each AK-SM800A unit and check the firmware version shown in the device's system information screen.
- Record the version for every unit in scope; the CVE record lists all versions before 3.3 as affected.

Step 2: Restrict login access on affected units

- Remove or disable any accounts not needed for immediate operations.
- Ensure the management interface is not reachable from untrusted network segments while the firmware update is arranged.

Step 3: Apply the firmware update

- Contact Danfoss to obtain firmware that moves each unit to version 3.3 or later; the record lists versions before 3.3 as affected.
- No vendor advisory was readable; confirm with Danfoss which release addresses CVE-2023-25915 before applying.

Step 4: Check for signs of unexpected activity

- Review device logs for commands or configuration changes made outside normal maintenance windows.
- Look for login events from unrecognised accounts or unusual times, particularly on units that were exposed before patching.

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 are writing regarding CVE-2023-25915, which affects the Danfoss AK-SM 800A Series (AK-SM800A). CISA has listed this with a remediation deadline of 28 November 2026. The flaw allows an authenticated remote user to run arbitrary commands; the CVE record lists all firmware versions before 3.3 as affected. We would like to know: whether we operate any AK-SM800A units; which firmware version each is running; whether version 3.3 or a later release confirmed by Danfoss addresses this CVE; and a plan and date for the update. Please provide written confirmation of the firmware version on each unit and the fix applied, by 27 November 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 commands or configuration changes in device logs, particularly outside normal maintenance windows.
- Login events from accounts or IP addresses not recognised as authorised administrators.
- Unusual outbound network connections originating from the device following a user login event.

The weakness behind it

The record classes this as CWE-20 (Improper Input Validation).

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
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 flaw requires remote authenticated access; an attacker would likely reach the device through its remote management interface, which is an external remote service.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The record states the flaw allows arbitrary command execution on the target; this would typically map to command interpreter use once the authenticated session is established.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	A near-maximum score on a command-execution flaw suggests the commands likely run with elevated privileges on the device, which would constitute privilege escalation.

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 input validation vulnerability that could allow a remote attacker to run arbitrary commands on the affected system.*

The CVE record, published by DIVD on 21 August 2023:

> *Due to improper input validation, an authenticated remote attacker could execute arbitrary commands on the target system.*

Versions of Danfoss AK-SM800A the record lists as affected:

- < 3.3

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-2023-25915
```

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-2023-25915
```

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

- No vendor advisory was readable; whether Danfoss has published a workaround or a specific patched release is not known from the available sources.
- The specific input field or interface that is vulnerable is not stated in the record.
- The record does not state whether version 3.3 is confirmed by Danfoss as the fixed release or whether a later version is required.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 25 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "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-2023-25915: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/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	Low	No special conditions beyond the flaw itself.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
21 August 2023	CVE record published by DIVD.
25 November 2026	CISA added it to its list of exploited vulnerabilities.
28 November 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
AK-SM800A on firmware before 3.3, management interface reachable by multiple users over a network	High	Before 28 November 2026
AK-SM800A on firmware before 3.3, single administrator account, internal network only	Medium	Before 28 November 2026
AK-SM800A on firmware before 3.3, no network access at all	Low	Next scheduled maintenance window

AK-SM800A on firmware 3.3 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-2023-25915: https://www.cve.org/CVERecord?id=CVE-2023-25915
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: csirt.divd.nl: https://csirt.divd.nl/CVE-2023-25915
- Reference in the CVE record: csirt.divd.nl: https://csirt.divd.nl/DIVD-2023-00025