contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Danfoss AK-SM 800A Series exploited

CVE-2023-25914 · on CISA's exploited list since 25 November 2026

Analysis Report

Organisations running Danfoss AK-SM800A firmware below version 3.3 must act before 28 November 2026. Start by locating every unit on your estate and checking its firmware version.

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.8**	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-2023-25914

The bottom line

> *Organisations running Danfoss AK-SM800A firmware below version 3.3 must act before 28 November 2026. Start by locating every unit on your estate and checking its firmware version.*

At a glance

Fact	Detail
Product	Danfoss AK-SM 800A Series (CVE-2023-25914)
Severity	High: 8.8 (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 record lists affected versions as below 3.3 for AK-SM800A, placing 3.3 as the boundary. No vendor advisory was readable to confirm which release carries the fix.
Who looks first	Anyone operating a Danfoss AK-SM 800A Series controller on firmware below version 3.3. The attacker must hold valid credentials, so the risk is highest where login access is shared or not tightly controlled.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you operate any Danfoss AK-SM 800A Series system controllers?	Nothing to do for this CVE.	Check the firmware version on each unit.
Is any unit running firmware below version 3.3?	No action needed on those units for this CVE.	Assess who can log in and contact Danfoss for the update.
Can more than one or two people log in to the affected unit?	Lower exposure; still apply the fix within the CISA window.	Restrict login access immediately while arranging the update.

What it is

An attacker who is already logged in to an AK-SM800A controller can use its XML interface to read files anywhere on the underlying server. The record says the information exposed can lead to a full system compromise.

Why it matters

Path traversal on a system controller can expose configuration files, stored credentials, or private keys on the underlying server. The record says the information read can lead to a full system compromise. Our reading is that credentials extracted from the device could allow access to other systems on the same network, so the impact is not confined to the controller. The CVSS score of 8.8 reflects the breadth of files reachable once logged in; login is required, which is the principal barrier.

Things people will get wrong

- It requires a login, so an outsider cannot exploit it. Authentication is a barrier, not a defence: any user who can log in — including an insider or someone holding stolen credentials — can run the exploit. The record confirms only authentication is needed.
- It only reads files, so the damage is limited. The record explicitly states the information read can lead to a full system compromise. Files such as credential stores or keys can enable further access well beyond the controller.

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 controller and locate the firmware version in the system information or about screen.
- Record the version for every unit. The record says versions below 3.3 are affected.

Step 2: Restrict login access on affected units

- Review who holds active credentials for each unit on a version below 3.3.
- Suspend or remove accounts that are not needed while the firmware update is arranged; this reduces the number of users who could trigger the flaw.

Step 3: Apply vendor mitigations or update firmware

- CISA's required action is to apply mitigations in accordance with vendor instructions. Contact Danfoss or your maintenance provider for the update package and confirmed fixed version.
- No vendor advisory was readable at the time this note was written; ask Danfoss to confirm the fixed release and any available workaround in writing.

Step 4: Check for signs of unexpected file access

- Review any available access or authentication logs on the controller for unusual login activity or unexpected XML interface requests around or before 25 November 2026.
- Look for access attempts referencing file paths outside the expected application area, such as paths containing double-dot sequences or absolute system paths.

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 about CVE-2023-25914, a path traversal vulnerability in the Danfoss AK-SM 800A Series controller affecting firmware below version 3.3. CISA has listed this as a known-exploited vulnerability with a remediation deadline of 28 November 2026. We need to establish whether we run any AK-SM800A units, which firmware version each unit is on, and whether the XML interface is accessible to more than a small number of trusted administrators. Please confirm in writing by 27 November 2026 the firmware version on each unit, whether any units fall below version 3.3, and what update or mitigation Danfoss recommends and when it can be applied.*

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:

- Unusual or repeated authentication events on the controller, particularly from accounts that do not normally use the XML interface.
- Requests to the XML interface referencing file paths that contain double-dot sequences or point outside the expected application directory.

The weakness behind it

The record classes this as CWE-22 (Improper Limitation of a Pathname to a Restricted Directory).

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
File and Directory Discovery (T1083): Listing files and folders to find what is there.	Discovery: looking around	Path traversal via the XML interface would likely be used to enumerate and read server files, which is consistent with file and directory discovery as an early step toward full compromise.
Data from Local System (T1005): Copying data stored on the machine.	Collection: gathering data	The record says system files of the underlying server can be read; collecting local data such as configuration files is the direct outcome the description describes.
Unsecured Credentials: Credentials In Files (T1552.001): Finding passwords or keys left in files.	Credential Access: stealing logins	Reading arbitrary server files would likely target credential files stored on the system, consistent with the record's warning that full compromise can follow from the information exposed.

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 a path traversal vulnerability that could allow an attacker to access and read underlying server system files via the XML interface.*

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

> *Due to improper restriction, authenticated attackers could retrieve and read system files of the underlying server through the XML interface. The information that can be read can lead to a full system compromise.*

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-2023-25914
```

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-2023-25914
```

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; it is not confirmed from a vendor source which release carries the fix or whether a workaround is available.
- The record does not specify which files or directories on the server are reachable through the XML interface.
- It is not stated whether the XML interface can be disabled or restricted as a temporary measure on affected firmware.
- 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", "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-2023-25914: score 8.8, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/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	Unchanged	Damage stays inside 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 below version 3.3, XML interface reachable, login shared across multiple users	High	Before 28 November 2026
AK-SM800A below version 3.3, login restricted to one or two known administrators	Medium	Before 28 November 2026
AK-SM800A below version 3.3, controller isolated from other networks	Medium	This week

AK-SM800A on version 3.3 or above	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-2023-25914: https://www.cve.org/CVERecord?id=CVE-2023-25914
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: csirt.divd.nl: https://csirt.divd.nl/CVE-2023-25914
- Reference in the CVE record: csirt.divd.nl: https://csirt.divd.nl/DIVD-2023-00025