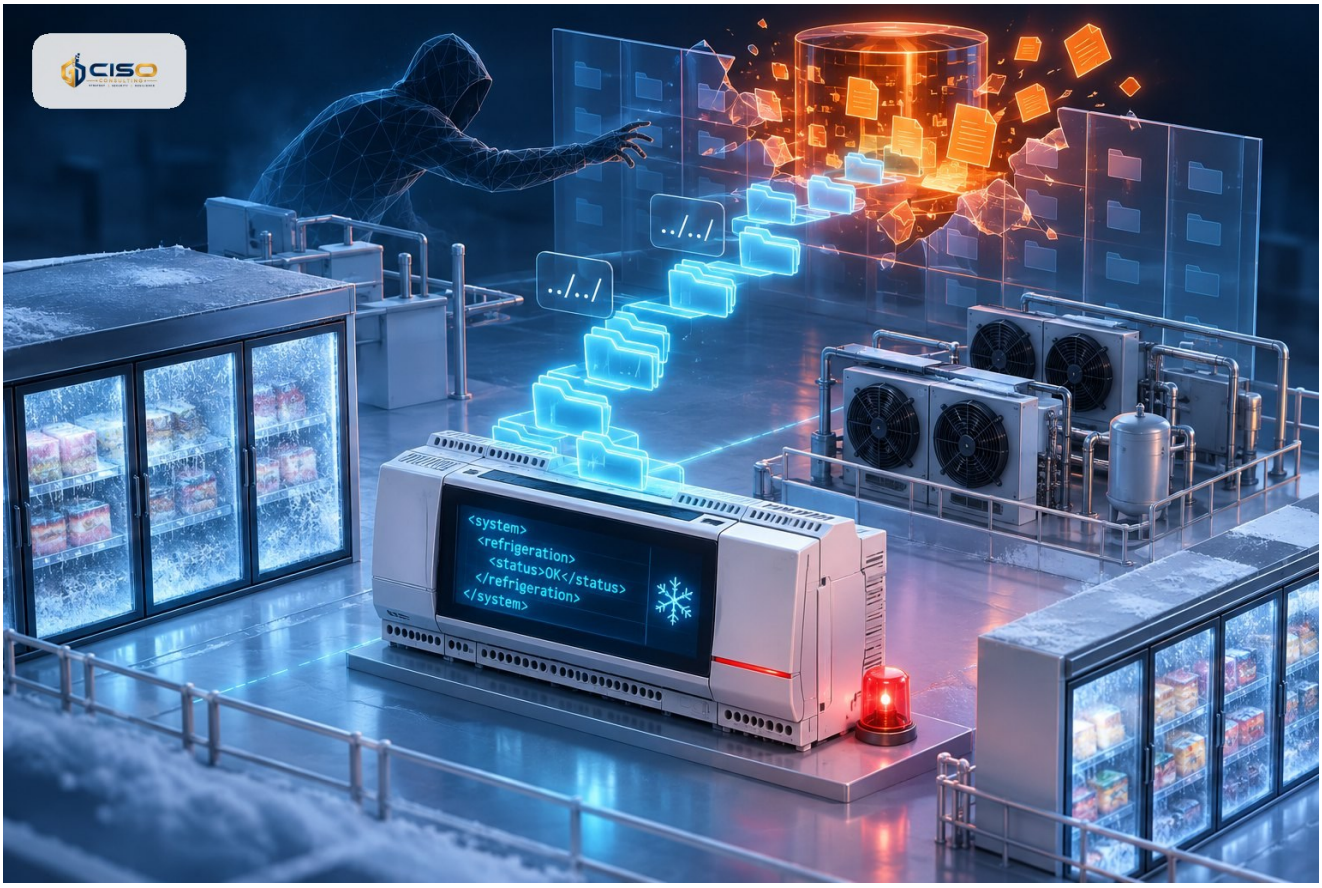
CISA flags path traversal flaw in Danfoss AK-SM 800A Series (CVE-2023-25914)



CISA lists CVE-2023-25914, a path traversal flaw in Danfoss AK-SM 800A Series that lets an attacker read server system files through the XML interface. Apply vendor mitigations or stop using the product.

- CVE-2023-25914 is a path traversal vulnerability in Danfoss AK-SM 800A Series.
- An attacker could read underlying server system files via the XML interface.
- CISA requires mitigations per vendor instructions, in line with BOD 26-04 and its Forensics Triage Requirements.
- If no mitigation exists, the product should be discontinued.
- The federal due date is 2026-11-28; asset owners must assess each asset's internet exposure.

What was reported

CISA has listed CVE-2023-25914, a **path traversal** vulnerability in the Danfoss AK-SM 800A Series. According to the entry, an attacker could access and read underlying server system files through the product's XML interface.

What CISA requires

The required action is to apply mitigations in accordance with the vendor's instructions, consistent with CISA's BOD 26-04 guidance on prioritizing security updates based on risk and its Forensics Triage Requirements. Where mitigations are not available, the product should be discontinued. For cloud services, the applicable BOD 26-04 guidance should be followed. The federal due date is 2026-11-28.

Stakeholders are responsible for assessing the internet exposure of each asset and for adhering to the BOD 26-04 patching guidelines. The source does not give further technical detail, affected versions or exploitation specifics, so teams should consult the vendor's instructions.

Implication for Saudi institutions

The CISA deadline applies to US federal bodies, but the guidance is a sensible reference for any organisation operating these devices. Start by confirming whether AK-SM 800A units exist in your estate, who manages them, and whether their interfaces can be reached from outside the internal network.

What to do now

1. Inventory all Danfoss AK-SM 800A Series units, including those at branches and facilities.
2. Check whether their web and XML interfaces are reachable from the internet or untrusted segments, and restrict access.
3. Obtain and apply the vendor's mitigation instructions.
4. Plan to retire the product if the vendor offers no mitigation.
5. Review device and server logs for unexpected file access and keep evidence in line with your incident procedures.