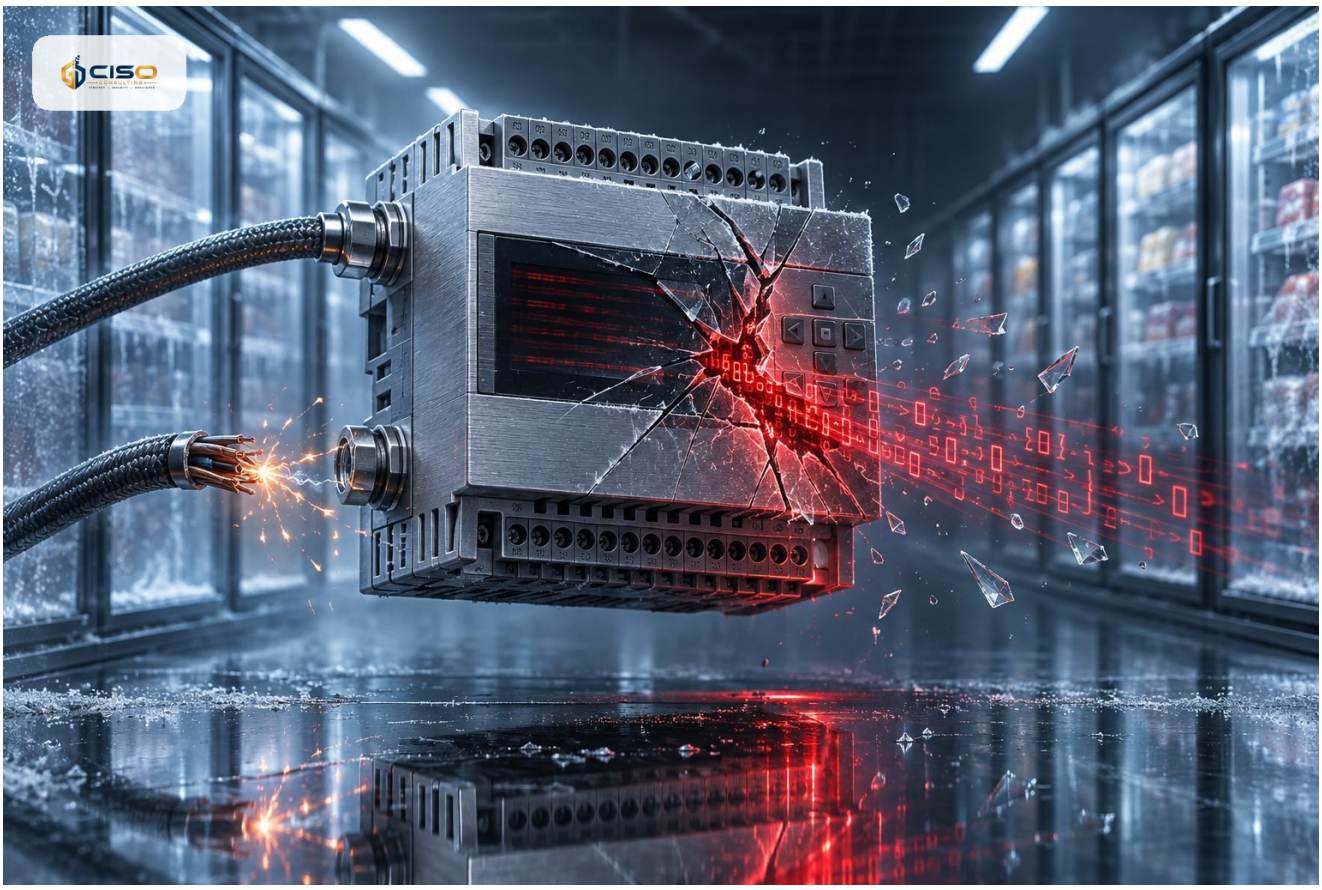
CISA flags CVE-2023-25915 in Danfoss AK-SM 800A Series allowing remote command execution



CISA lists an improper input validation flaw, CVE-2023-25915, in Danfoss AK-SM 800A Series that could let a remote attacker run arbitrary commands. Operators should apply vendor mitigations or stop using the product.

- CVE-2023-25915 is an improper input validation vulnerability in Danfoss AK-SM 800A Series.
- A remote attacker could run arbitrary commands on the affected system.
- CISA requires mitigations per vendor instructions, in line with BOD 26-04 and its Forensics Triage Requirements.
- If mitigations are unavailable, use of the product should be discontinued.
- The federal due date is 2026-11-28; asset owners must assess each asset's internet exposure.

CISA has listed CVE-2023-25915, an improper input validation vulnerability in the Danfoss AK-SM 800A Series. According to the entry, a remote attacker could exploit it to run arbitrary commands on the affected system.

What CISA requires

CISA directs affected stakeholders to apply mitigations following the vendor's instructions, and to do so in line with its BOD 26-04 guidance on prioritizing security updates based on risk. It also points to its Forensics Triage Requirements. Where cloud services are involved, the applicable BOD 26-04 guidance should be followed. If no mitigations are available, the product should no longer be used.

The federal due date is 2026-11-28. That deadline binds US federal agencies, but it is a useful reference point for any organization planning its own response.

What it means for Saudi institutions

The source does not describe deployments in the Kingdom, so the first task is to establish whether the product is present at all. Organizations that run AK-SM 800A Series units should treat the issue as one of exposure: stakeholders are responsible for judging how reachable each asset is from the internet and for keeping to the patching expectations in BOD 26-04.

The source gives no details on affected versions, fixes or exploitation, so rely on the vendor's own instructions for those specifics.

What to do now

1. Check asset inventories and building or facility systems for Danfoss AK-SM 800A Series units.
2. Determine whether each unit is reachable from the internet and restrict that access where it is not essential.
3. Apply mitigations following the vendor's instructions and record the work.
4. If no mitigation is available, plan to retire or replace the product.
5. Review logs and, where exposure existed, perform forensic triage for signs of unauthorized command execution.