Danfoss A/S
DK-6430 Nordborg
CVR No.: 20 16 57 15

E-mail: danfoss@danfoss.com
Homepage: www.danfoss.com

November 3, 2026

AK-System Manager – Cybersecurity Incident in Europe – klant informatie

Geachte klant,

Verschillende locaties in Europa hebben verdachte veranderingen gemeld in de vroege uren van 2 november, waaronder ongewoon hoge ontdooitemperaturen, gewijzigde temperatuurinstellingen en het activeren van elektrische ontdooiing.

Bekende getroffen Danfoss-systemen waren direct blootgesteld aan het openbare internet (zonder VPN, niet werkend achter een firewall).

De getroffen apparatuur bij de gemelde incidenten was:

1. Uitloopproducten AK-SM800 en AK-SC355 systemen
2. AK-SM800A-systemen die werken op verouderde softwareversies

Aanbevolen noodmaatregelen
(zie details over verplichte vereisten en best practices op de volgende pagina):

1. Verwijder de internetblootstelling van getroffen units en van alle units die openbaar IP-eigendom zijn
2. Herstel en verifieer de volledige configuratie
3. Update de huidige generatie AK-SM800A-systemen naar de nieuwste beschikbare firmwareversie
4. Schakel Strikte Modus in op de AK-SM800A
5. Herstel de toegang tot de units alleen via een beveiligde VPN
   of in het algemeen via een beveiligd netwerk

Voor verdere technische ondersteuning kunt u contact opnemen met het regionale technische ondersteuningsteam.

Danfoss raadt bovendien aan om de apparaten (AK-SC355, AK-SM800) te updaten naar producten van de huidige generatie (AK-SM800A-serie), om te zorgen voor continue cyberbeveiligingsupdates.

Danfoss blijft de situatie volgen en blijft zich volledig inzetten om onze klanten te ondersteunen tijdens deze moeilijke situatie.

Deel deze informatie ook met uw klanten en eindgebruikers in de supermarkt om ervoor te zorgen dat alle relevante sites geïnformeerd zijn en de aanbevolen noodmaatregelen kunnen nemen.

Met vriendelijke groet,

Jonas Hildebrandt | Senior Director Product Management
Electronic Controllers & Services | Danfoss Climate Solutions
jonas.hildebrandt@danfoss.com | Mobile: +49 151 2626 4387

AK-Systeemmanager Cybersecurity: Verplichte vereisten en aanbevolen best practices

Cyberbeveiliging - verplichte vereisten

Danfoss beschouwt de volgende aspecten als verplicht bij het plannen om uw System Manager aan te sluiten op digitale netwerken.
Het niet implementeren van de onderstaande verplichte vereisten stelt je System Manager en aangesloten applicaties bloot aan kwaadaardige aanvallen en valt buiten de door Danfoss aanbevolen bedrijfsstand.

AK-SC355 (uit de verkoop genomen in 2016, vervangen door de AK-SM800)

- Verbind een Systeembeheerder niet direct met openbaar internet of onbetrouwbare open netwerken
- Bescherm externe toegang met een veilige VPN die achter een stateful firewall is beëindigd met een denybydefault-beleid
- Zorg ervoor dat fabrieksgebruiker en wachtwoord zijn gewijzigd

AK-SM800 (uit de verkoop in 2023, vervangen door de AK-SM800A)

- Verbind een Systeembeheerder niet direct met openbaar internet of onbetrouwbare open netwerken
- Bescherm externe toegang met een veilige VPN die achter een stateful firewall is beëindigd met een denybydefault-beleid
- Zorg ervoor dat fabrieksgebruiker en wachtwoord zijn gewijzigd

AK-SM800A (wereldwijd actief verkocht en ondersteund)

- Verbind een System Manager niet direct met het publieke internet of onbetrouwbare open netwerken
- Bescherm externe toegang met een veilige VPN die achter een stateful firewall is beëindigd met een denybydefault-beleid
- Zorg ervoor dat System Manager de nieuwste softwareversie draait om cyberbeveiligingsfunctionaliteit te maximaliseren
- Zorg ervoor dat het beveiligingsniveau van de Systeembeheerder op **Strict-modus** is gezet (Configuration>Security-Strict)

Cyberbeveiliging - best practices (volg deze best practices naast de verplichte vereisten)

- Wachtwoorden regelmatig wijzigen en niet delen of publiceren
- Standaardbeheerpoorten wijzigen of de toegang beperken tot alleen toegestane bronnen
- Het besturingsnetwerk segmenteren (bijv. VLAN's); Isoleren van bedrijfs- en gastnetwerken
- Configuraties veilig back-uppen
- Raadpleeg beschikbare industrienormen (i.e. ISO/IEC 27002:2013) voor verdere referentie en richtlijnen