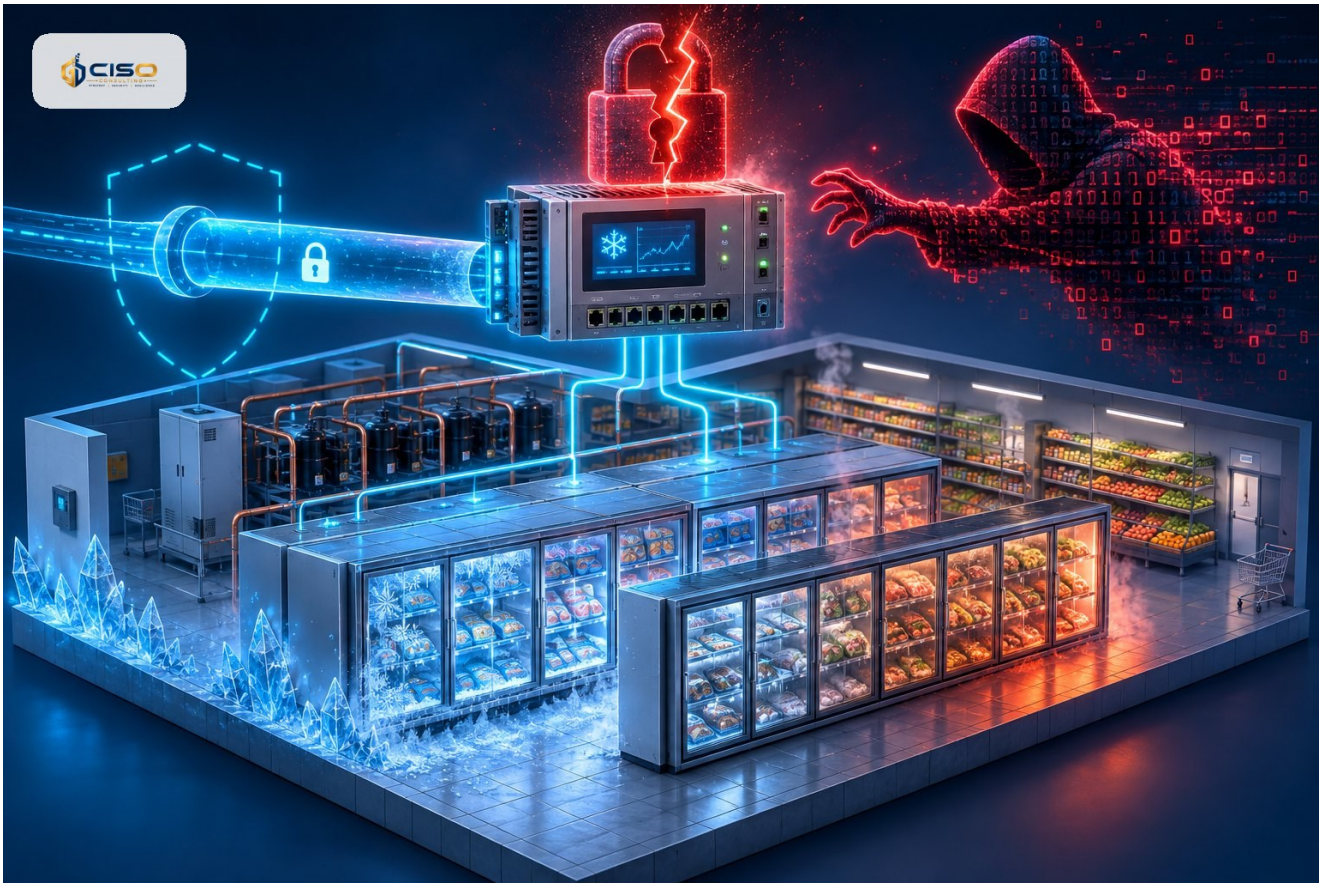
CISA تحذّر من ثغرة حرجة غير مصحَّحة في وحدات التحكم بالتبريد Danfoss AK-SM 8xxA



تحذّر CISA من الثغرة CVE-2026-129713 (بدرجة 9.8) في وحدات Danfoss AK-SM 8xxA التي تتيح هجمات دون مصادقة وربما تنفيذ تعليمات عن بُعد. لا توجد تصحيحات بعد، ويُنصح بالعزل والوصول عبر VPN فقط.

- CVE-2026-129713 ثغرة تجاوز سعة مكدس في خادم وحدات Danfoss AK-SM 8xxA بدرجة 9.8.
- يمكن لمهاجم دون مصادقة إعادة تشغيل الخادم وربما تنفيذ تعليمات بصلاحيات خادم الويب.
- تعتزم Danfoss معالجتها في الإصدار x.5.5، ولا يتوافر تصحيح حاليًا.
- تدير هذه الوحدات التبريد في قطاع تجزئة الأغذية، وفي بعض الطرازات الإضاءة وتكييف الهواء.
- استُهدفت وحدات Danfoss مؤخرًا في هجمات على متاجر أوروبية أدت إلى إيقاف التبريد أو تغيير إعداداته.

حذّرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) من ثغرة حرجة في وحدات التحكم Danfoss AK-SM 8xxA Series التي تستخدمها متاجر التجزئة الغذائية لإدارة التبريد التجاري، وكذلك الإضاءة وتكييف الهواء في بعض الطرازات.

تفاصيل الثغرة

تحمل الثغرة المعرّف **CVE-2026-129713** ودرجة خطورة 9.8، وهي تجاوز لسعة المكدس في خادم وحدة التحكم. وبحسب CISA، لا يحتاج المهاجم إلى مصادقة لاستغلالها، ويمكنه إعادة تشغيل الخادم، وقد يتمكن من تنفيذ تعليمات عن بُعد بصلاحيات خادم الويب. وتشمل الثغرة سلسلة AK-SM 800A بطرازاتها 820A و850A و880A. وتشير CISA إلى انتشار هذه الأجهزة عالميًا دون وضوح عددها.

الوضع الحالي والسياق

نشرت Danfoss في 20 نوفمبر إشعارًا أمنيًا يفيد بمعالجة المشكلة في الإصدار x.5.5 القادم، الذي سيزيل كذلك خيار تعطيل «Strict mode». ولا يتوافر تصحيح حاليًا.

ويأتي التحذير بعد حوادث حديثة في أوروبا اختُرقت فيها وحدات تحكم تبريد، منها Danfoss، في متاجر كبرى، فتوقف التبريد أو عُدّلت إعداداته. كما أُفيد باستهداف مورّد تبريد لخدمة نقل الدم الفرنسية وتغيير إعدادات التخزين البارد.

إجراءات مؤقتة

إلى حين صدور التصحيح، توصي CISA بإبعاد الوحدات عن الإنترنت العام وتقليل انكشافها على الشبكة، وفصل أنظمة التحكم عن شبكات الأعمال خلف جدران حماية، واستخدام شبكات VPN محدّثة عند الحاجة إلى الوصول عن بُعد.

ما يجب فعله الآن

1. حصر وحدات Danfoss AK-SM 8xxA (820A وA850 وA880) في المتاجر والمستودعات ومواقع سلسلة التبريد، بما فيها ما يديره مزوّدو المرافق من الأطراف الثالثة.
2. التأكد من عدم إمكانية الوصول إليها من الإنترنت العام وإزالة أي انكشاف مباشر.
3. فصل هذه الوحدات عن شبكات الأعمال خلف جدران حماية، وفق متطلبات الضوابط الأساسية للأمن السيبراني للأنظمة التشغيلية (NCA OTCC).
4. حصر الوصول عن بُعد في شبكات VPN محدّثة، ومراجعة السجلات الأخيرة بحثًا عن إعادة تشغيل غير متوقعة أو تغيّر في الإعدادات.
5. متابعة إشعار Danfoss والتخطيط لتطبيق الإصدار x.5.5 فور صدوره مع خطة اختبار ورجوع.
6. مطالبة موردي التبريد والمرافق بتأكيد انكشافهم والضوابط المؤقتة كتابيًا.