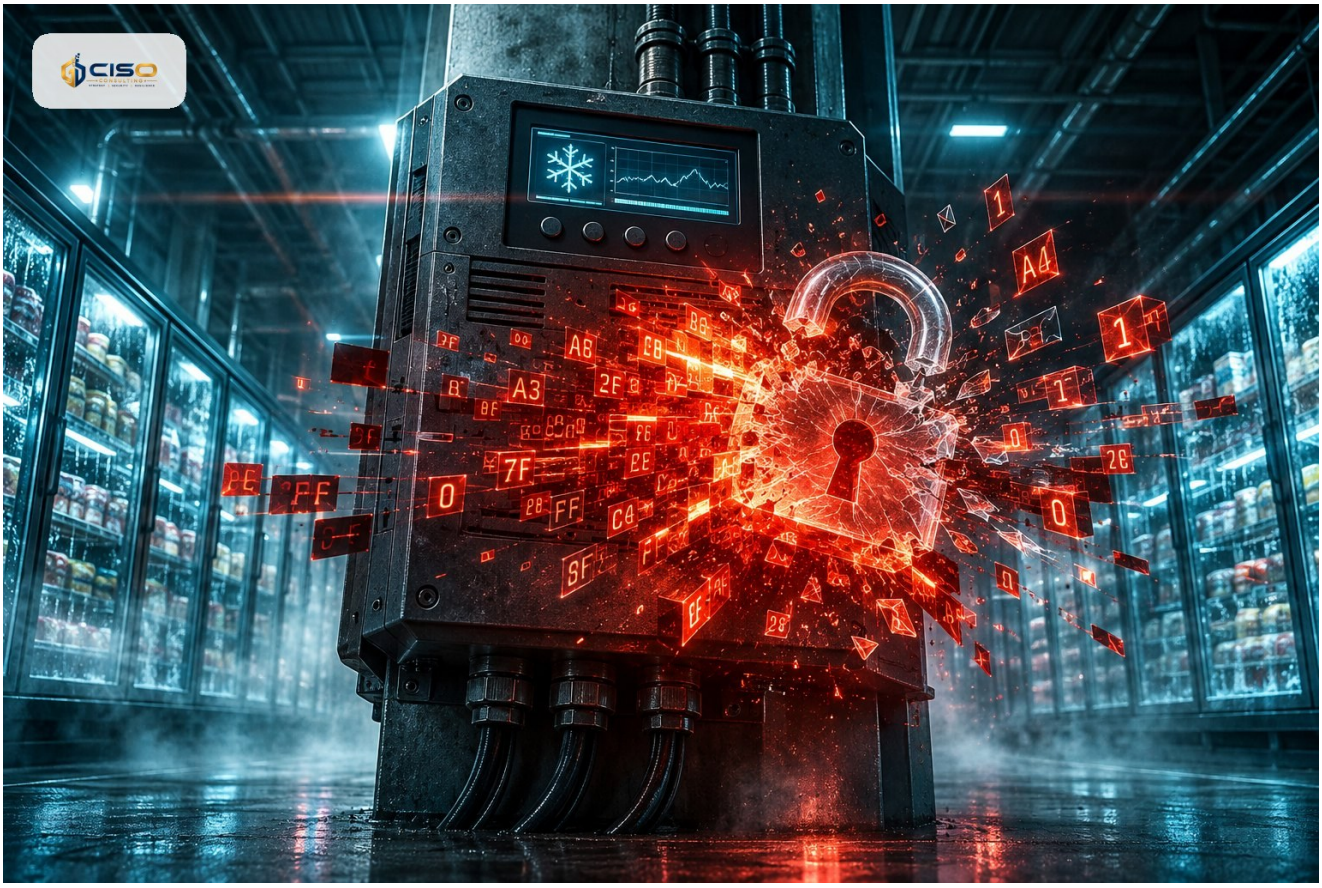
وحدات التحكم Danfoss AK-SM 8xxA: ثغرة تجاوز مخزن مؤقت دون مصادقة وفق CISA



أصدرت CISA تنبيهاً عن الثغرة CVE-2026-129713 (CVSS v3 بدرجة 9.8) في وحدات Danfoss AK-SM 8xxA حتى الإصدار 5.4.0، والإصلاح مخطط له في الإصدار x.5.5.

- الثغرة CVE-2026-129713 هي تجاوز مخزن مؤقت في المكدس داخل معالج CGI لا يتطلب مصادقة.
- المتأثر: Danfoss AK-SM8xxA بالإصدار 5.4.0 وما قبله، بدرجة CVSS v3 تبلغ 9.8.
- طلبات HTTP/S POST مصممة خصيصاً قد تتلف الذاكرة وتعيد تشغيل خادم الويب، مع احتمال تنفيذ شيفرة بصلاحيات خادم الويب.
- لا يلزم أي تصريح دخول لاستغلالها.
- تخطط Danfoss لمعالجتها في الإصدار x.5.5 وستزيل خيار تعطيل Strict Mode في إصدارات لاحقة.

ما الذي ورد في التنبيه

نشرت CISA تنبيهاً خاصاً بأنظمة التحكم الصناعي يتناول سلسلة Danfoss AK-SM 8xxA، وهي وحدات تحكم تُستخدم في المنشآت التجارية. الثغرة، ورقمها CVE-2026-129713، تجاوز مخزن مؤقت في المكدس داخل معالج CGI لا يتطلب مصادقة، وتبلغ درجتها 9.8 وفق CVSS v3.

يمكن لمهاجم يصل إلى الجهاز إرسال طلبات HTTP/S POST مصممة خصيصاً. ويصف التنبيه تلفاً في الذاكرة وإعادة تشغيل لخادم الويب، مع احتمال تنفيذ شيفرة عشوائية بصلاحيات خادم الويب. والإصدارات المتأثرة هي 5.4.0 وما قبله.

استجابة المورّد

تذكر Danfoss أن المشكلة ستُعالج في إصدار برمجي قادم لسلسلة AK-SM 800A هو x.5.5. كما تعتزم إزالة إمكانية تعطيل Strict Mode من المستخدمين في إصدارات مقبلة. ولا يذكر المصدر وجود تحديث متاح حالياً ولا رصد استغلال فعلي.

الأثر على الجهات المشغِّلة

ينبغي للجهات التي تشغّل هذه الوحدات في مبانٍ تجارية، مثل المتاجر ومخازن التبريد وإدارة المرافق، التعامل مع الثغرة بجدية لأنها لا تحتاج إلى بيانات اعتماد. وإلى حين صدور إصدار مُصحَّح، فإن تقليل إمكانية الوصول الشبكي إلى واجهة الويب هو الإجراء الأكثر عملية.

- حصر وحدات AK-SM 8xxA وإصداراتها.
- التأكد من عدم إتاحتها من الإنترنت أو الشبكات غير الموثوقة.
- متابعة إعلانات Danfoss بشأن الإصدار x.5.5.

ما يجب فعله الآن

1. حصر جميع وحدات Danfoss AK-SM 8xxA وتسجيل إصدارات برمجياتها.
2. التحقق من عدم إتاحتها على الإنترنت وحصر الوصول إلى واجهة الويب في شبكات الإدارة الموثوقة.
3. وضع الوحدات خلف عزل شبكي وقواعد جدار ناري تقيّد HTTP/S بالأجهزة المعتمدة.
4. رصد إعادة تشغيل خادم الويب غير المتوقعة أو حركة POST غير المعتادة نحو هذه الأجهزة.
5. التخطيط للترقية إلى الإصدار x.5.5 فور صدوره ومتابعة إشعارات المورّد.