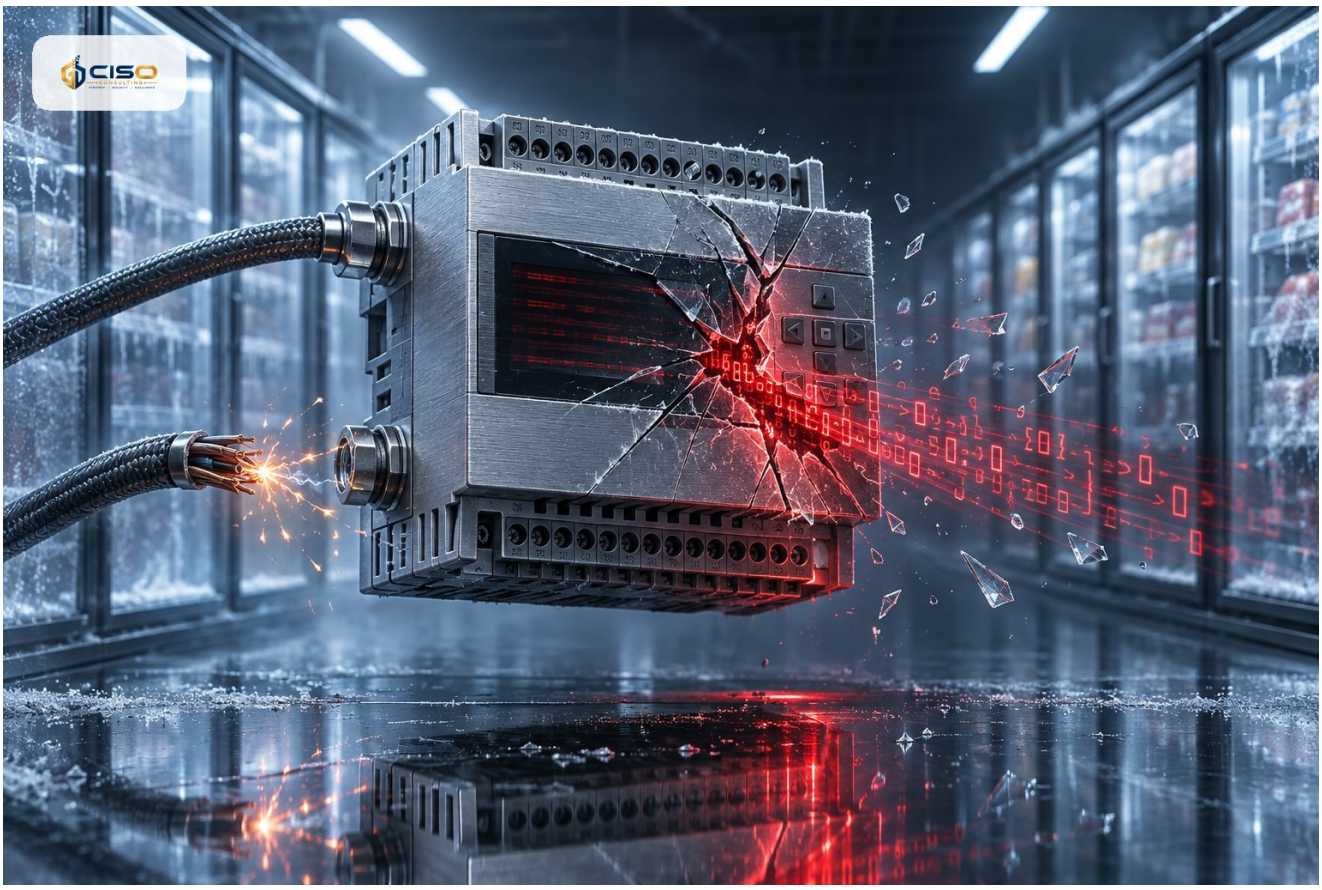
CISA تحذّر من الثغرة CVE-2023-25915 في Danfoss AK-SM 800A Series التي تتيح تنفيذ أوامر عن بُعد



أدرجت CISA الثغرة CVE-2023-25915 في Danfoss AK-SM 800A Series، وهي خلل في التحقق من المدخلات قد يتيح لمهاجم عن بُعد تنفيذ أوامر. يُنصح بتطبيق إجراءات المورّد أو إيقاف استخدام المنتج.

- CVE-2023-25915 ثغرة في التحقق من المدخلات تؤثر على Danfoss AK-SM 800A Series.
- قد يتمكن مهاجم عن بُعد من تنفيذ أوامر عشوائية على النظام المتأثر.
- تطلب CISA تطبيق إجراءات التخفيف وفق تعليمات المورّد وبما يتوافق مع BOD 26-04 ومتطلبات الفحص الجنائي الأولي.
- إذا لم تتوفر إجراءات تخفيف، يُوصى بإيقاف استخدام المنتج.
- الموعد النهائي للجهات الفيدرالية الأمريكية هو 28-11-2026، وعلى المالكين تقييم تعرّض كل أصل للإنترنت.

أدرجت CISA الثغرة CVE-2023-25915، وهي خلل في التحقق من المدخلات في Danfoss AK-SM 800A Series. وبحسب الإدراج، يمكن لمهاجم عن بُعد استغلالها لتنفيذ أوامر عشوائية على النظام المتأثر.

ما تطلبه CISA

توجّه CISA الجهات المعنية إلى تطبيق إجراءات التخفيف وفق تعليمات المورّد، وبما يتوافق مع إرشادات BOD 26-04 الخاصة بترتيب أولويات التحديثات الأمنية بحسب المخاطر، كما تشير إلى متطلبات الفحص الجنائي الأولي (Forensics Triage Requirements). وعند وجود خدمات سحابية ينبغي اتباع إرشادات BOD 26-04 المنطبقة. وإذا لم تتوفر إجراءات تخفيف فيجب التوقف عن استخدام المنتج.

الموعد النهائي للجهات الفيدرالية الأمريكية هو 28-11-2026. وهو ملزم لتلك الجهات فقط، لكنه مرجع مفيد لأي منظمة تخطط لاستجابتها.

الأثر على المؤسسات في المملكة

لا تتناول المصدر أي عمليات تشغيل داخل المملكة، لذا فالخطوة الأولى هي التحقق من وجود المنتج أصلًا. وعلى المنظمات التي تشغّل وحدات AK-SM 800A Series التعامل مع المسألة بوصفها مسألة تعرّض: فالمسؤولية تقع على المالكين في تقييم مدى إمكانية الوصول إلى كل أصل من الإنترنت والالتزام بتوقعات التحديث الواردة في BOD 26-04.

لا يوضح المصدر الإصدارات المتأثرة أو الإصلاحات أو وقوع استغلال فعلي، لذا يُرجع في هذه التفاصيل إلى تعليمات المورّد.

ما يجب فعله الآن

1. مراجعة سجلات الأصول وأنظمة المباني والمرافق بحثاً عن وحدات Danfoss AK-SM 800A Series.
2. تحديد ما إذا كانت كل وحدة متاحة من الإنترنت، وتقييد هذا الوصول إن لم يكن ضرورياً.
3. تطبيق إجراءات التخفيف وفق تعليمات المورّد وتوثيق ما يتم.
4. إذا لم تتوفر إجراءات تخفيف، التخطيط لإيقاف المنتج أو استبداله.
5. مراجعة السجلات، وعند وجود تعرّض سابق إجراء فحص جنائي أولي بحثاً عن تنفيذ أوامر غير مصرّح به.