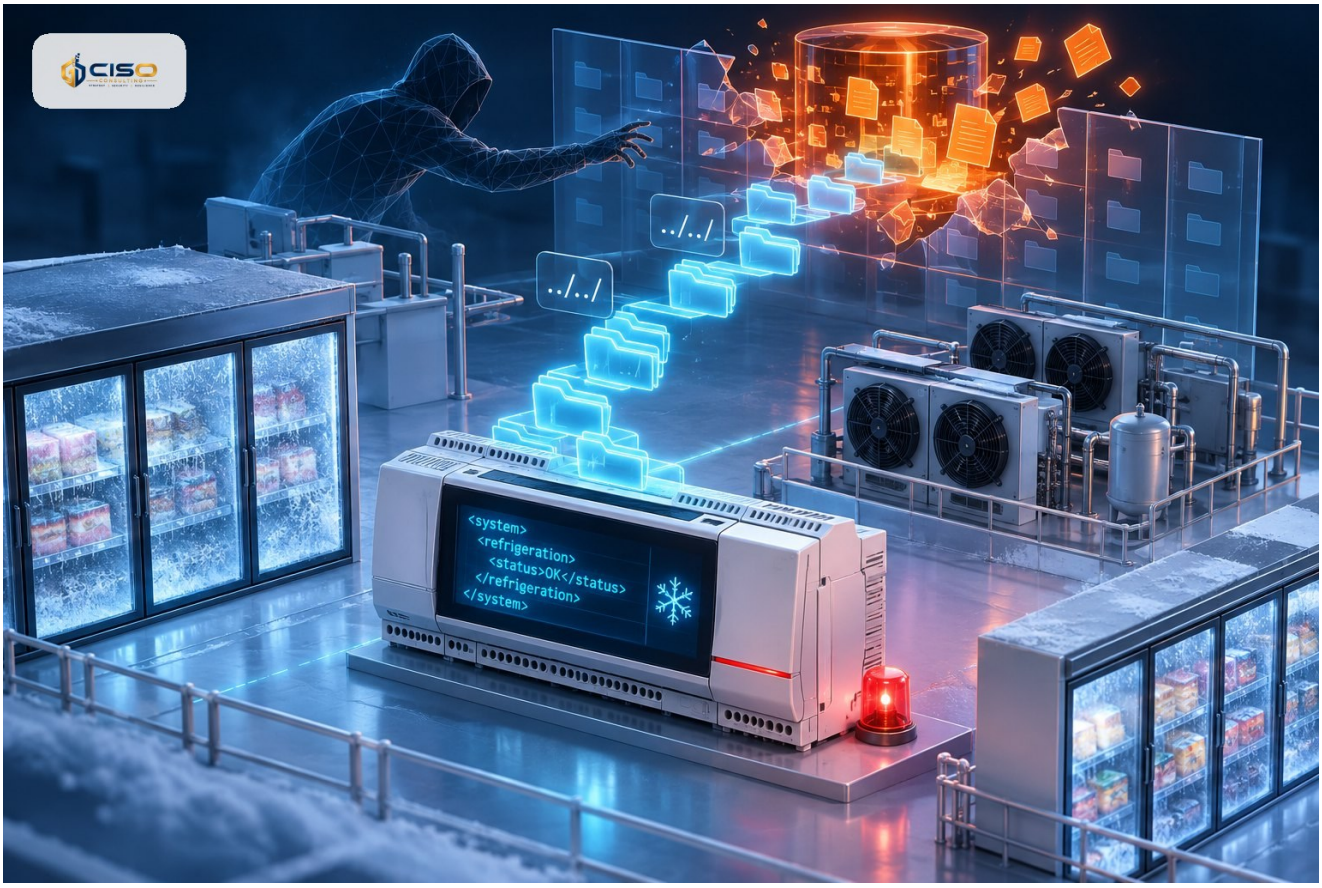
CISA تحذّر من ثغرة اجتياز مسار في Danfoss AK-SM 800A Series (CVE-2023-25914)



أدرجت CISA الثغرة CVE-2023-25914 في Danfoss AK-SM 800A Series، وهي اجتياز مسار يتيح قراءة ملفات النظام عبر واجهة XML. يلزم تطبيق معالجات المورّد أو التوقف عن استخدام المنتج.

- CVE-2023-25914 ثغرة اجتياز مسار في Danfoss AK-SM 800A Series.
- قد يتمكن المهاجم من قراءة ملفات نظام الخادم عبر واجهة XML.
- تشترط CISA تطبيق المعالجات وفق تعليمات المورّد، بما يتوافق مع BOD 26-04 ومتطلبات Forensics Triage.
- إذا لم تتوفر معالجة فيجب التوقف عن استخدام المنتج.
- الموعد النهائي للجهات الفيدرالية الأمريكية هو 28-11-2026، وعلى مالكي الأصول تقييم تعرّض كل أصل للإنترنت.

ما الذي أُعلن

أدرجت CISA الثغرة CVE-2023-25914، وهي ثغرة **اجتياز مسار** في Danfoss AK-SM 800A Series. ووفق الإدراج، يمكن للمهاجم الوصول إلى ملفات نظام الخادم الأساسية وقراءتها عبر واجهة XML الخاصة بالمنتج.

ما الذي تشترطه CISA

الإجراء المطلوب هو تطبيق المعالجات وفق تعليمات المورّد، بما ينسجم مع توجيه CISA BOD 26-04 بشأن ترتيب أولوية التحديثات الأمنية حسب المخاطر ومع متطلباتها الخاصة بـ Forensics Triage. وإذا لم تتوفر معالجات فيجب التوقف عن استخدام المنتج. أما الخدمات السحابية فيُتّبع بشأنها التوجيه المنطبق في BOD 26-04. والموعد النهائي للجهات الفيدرالية الأمريكية هو 28-11-2026.

وتقع على عاتق الجهات المعنية مسؤولية تقييم تعرّض كل أصل للإنترنت والالتزام بإرشادات التحديث الواردة في BOD 26-04. ولا يتضمن المصدر تفاصيل تقنية إضافية أو إصدارات متأثرة أو معلومات عن الاستغلال، لذا ينبغي الرجوع إلى تعليمات المورّد.

الأثر على المؤسسات في المملكة

الموعد المذكور يخص الجهات الفيدرالية الأمريكية، لكن التوجيه مرجع مفيد لأي جهة تشغّل هذه الأجهزة. والبداية بالتحقق من وجود وحدات AK-SM 800A في بيئتكم، ومن المسؤول عنها، وهل يمكن الوصول إلى واجهاتها من خارج الشبكة الداخلية.

ما يجب فعله الآن

1. حصر جميع وحدات Danfoss AK-SM 800A Series في الفروع والمنشآت.
2. التحقق من إمكانية الوصول إلى واجهات الويب وXML من الإنترنت أو من شبكات غير موثوقة، وتقييد الوصول إليها.
3. الحصول على تعليمات المعالجة من المورّد وتطبيقها.
4. التخطيط لإيقاف استخدام المنتج إذا لم يوفر المورّد معالجة.
5. مراجعة سجلات الجهاز والخادم بحثًا عن وصول غير متوقع للملفات، والاحتفاظ بالأدلة وفق إجراءات الاستجابة للحوادث.