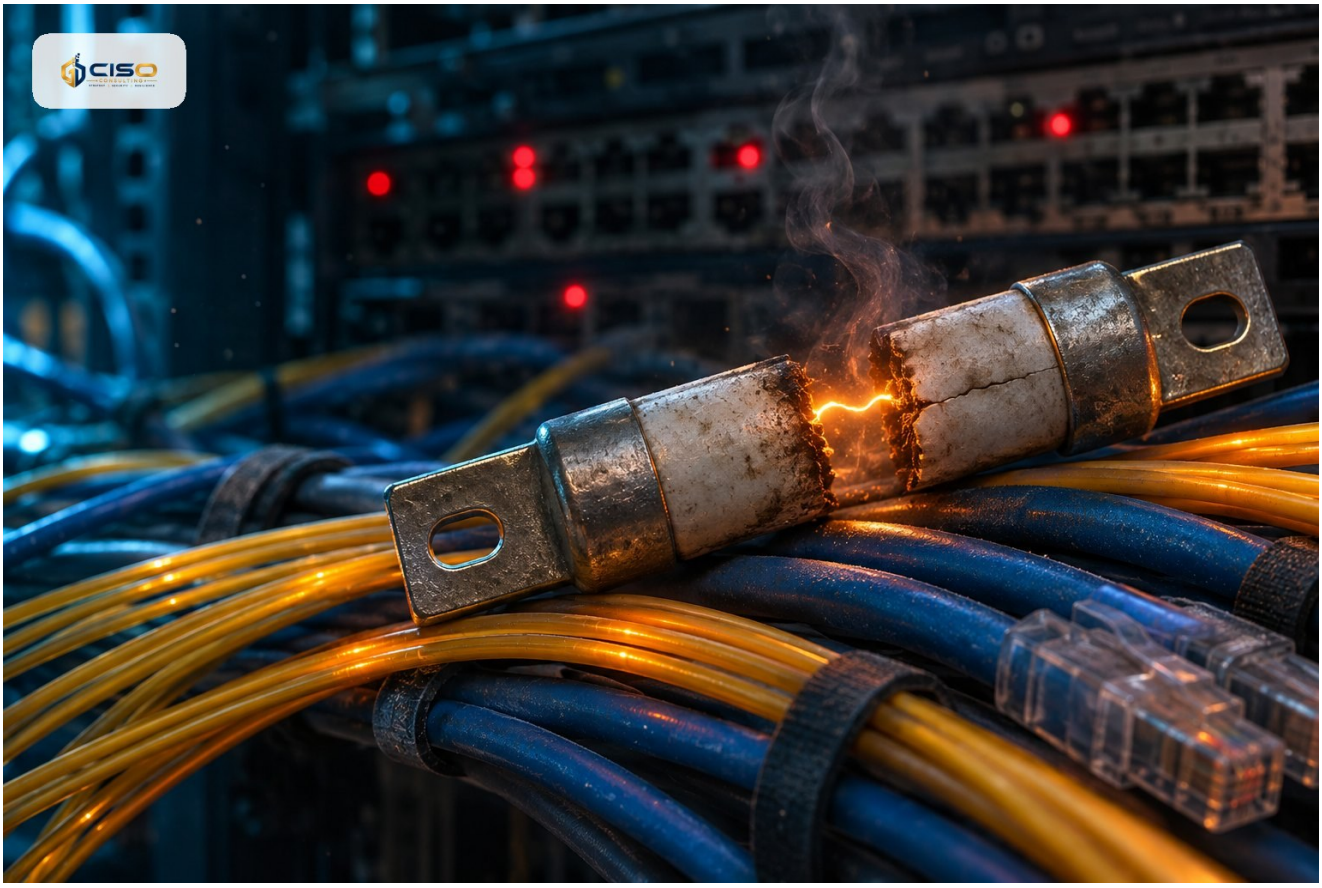
سيمنز SENTRON 3NA COM Fuse: ثغرة حجب خدمة (CVE-2024-7322) تؤثر على الإصدارات الأقدم من 5.2



نشرت CISA نشرة عن ثغرة حجب خدمة (CVE-2024-7322) في Siemens SENTRON 3NA COM Fuse للإصدارات الأقدم من 5.2، وقد يتطلب التعافي إعادة تأسيس الشبكة المتأثرة.

- المتأثر: إصدارات SENTRON 3NA COM Fuse الأقدم من V5.2.
- CVE-2024-7322 ثغرة حجب خدمة ناتجة عن تحقق غير سليم من مصدر قناة الاتصال.
- قد يغيّر جهاز ZigBee معرّف العقدة عند استلام رد انضمام مشفّر غير مطلوب، مما يسبب حجب الخدمة.
- قد يتطلب التعافي إعادة تأسيس الشبكة.
- درجة CVSS v3 المقدّمة من المورّد هي 5.8.

أصدرت CISA نشرة بشأن ثغرة حجب خدمة في Siemens SENTRON 3NA COM Fuse. تحمل الثغرة الرمز CVE-2024-7322 وتشمل جميع الإصدارات الأقدم من V5.2، وبلغت درجة CVSS v3 المقدّمة من المورّد 5.8.

طبيعة المشكلة

توصَّف الثغرة بأنها تحقق غير سليم من مصدر قناة الاتصال. فقد يغيّر منسّق ZigBee أو الموجّه أو الجهاز الطرفي معرّف العقدة عند استلام رد انضمام مشفّر لم يُطلب، ويؤدي هذا التغيير إلى حالة حجب خدمة.

وعند نجاح الاستغلال قد يلزم إعادة تأسيس الشبكة المتأثرة قبل عودة التشغيل الطبيعي.

أهمية الأمر

تذكر CISA أن المنتج منتشر عالميًا وأن مقر الشركة في ألمانيا، وتشير النشرة إلى قطاعات بنية تحتية حيوية عدة، منها التصنيع الحيوي والطاقة والرعاية الصحية والخدمات المالية والنقل والمرافق الحكومية. ولذلك ينبغي للجهات في المملكة التي تشغّل مراقبة توزيع كهربائي في هذه البيئات التحقق من وجود هذا المكوّن.

لا يتضمن المقتطف المتاح تفاصيل المعالجة، لذا يُرجع إلى نشرتي Siemens وCISA لمعرفة الإصدار المعالج وأي إجراءات تخفيف.

النهج المقترح

بما أن التقييم متوسط، فالاستجابة الهادئة والمخططة مناسبة: التأكد من التعرض، ومراجعة إرشادات المورّد، وجدولة التحديث ضمن إدارة التغيير المعتادة.

ما يجب فعله الآن

1. حصر أنظمة التقنية التشغيلية وأنظمة الطاقة في المباني بحثًا عن SENTRON 3NA COM Fuse وتسجيل الإصدار المثبّت.
2. تحديد الوحدات التي تعمل بإصدار أقدم من V5.2.
3. مراجعة نشرتي Siemens وCISA لمعرفة الإصدار المعالج وإجراءات التخفيف.
4. جدولة التحديث عبر إدارة التغيير مع التخطيط لاحتمال إعادة تأسيس الشبكة.
5. إعداد إجراء استعادة لشبكة ZigBee عند حدوث حجب الخدمة.