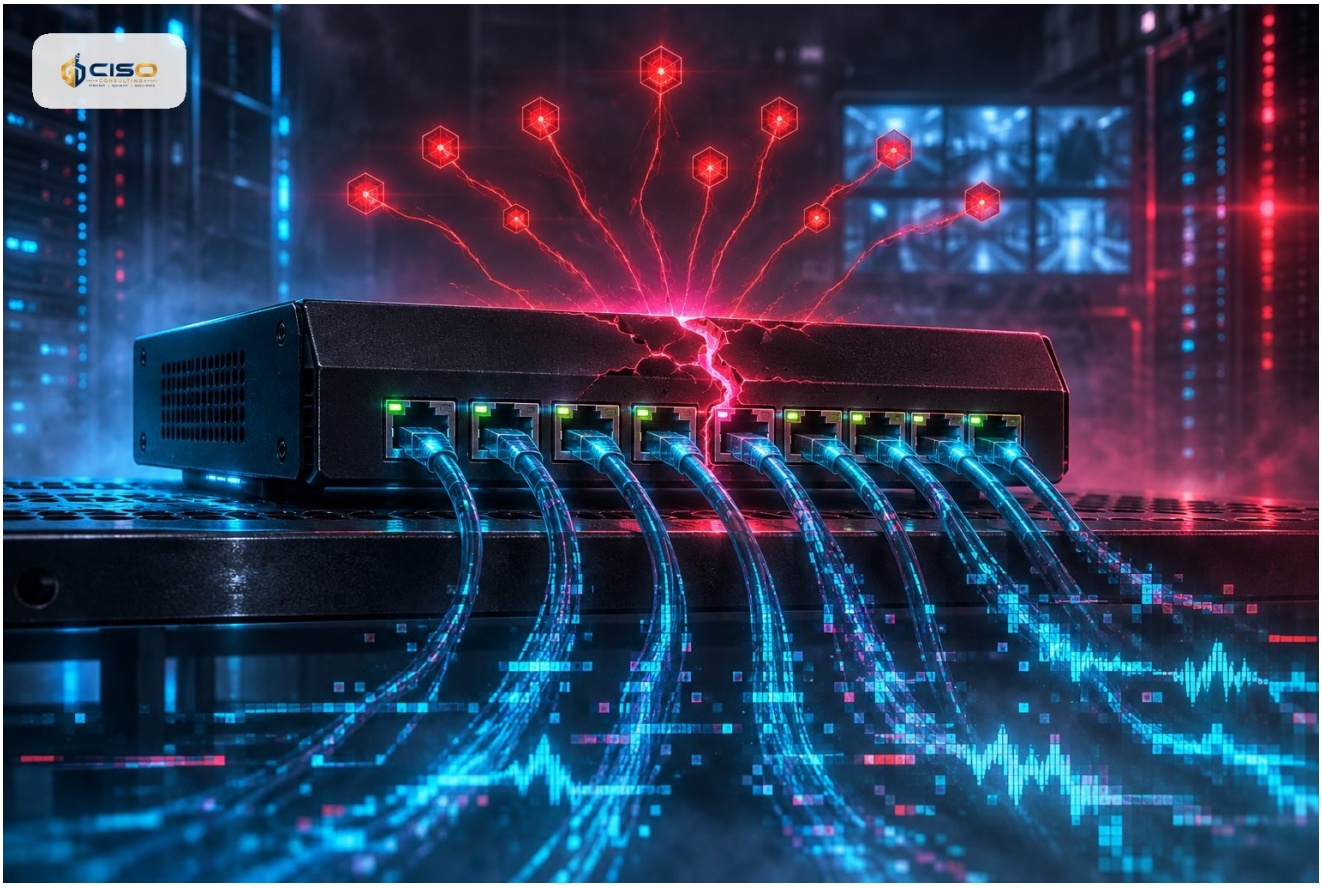
CISA تحذّر من ثغرات حرجة في البرنامج الثابت لجهاز Kiloview E3 NDI Encoder قبل الإصدار 1.30



نشرت CISA تنبيهاً بشأن البرنامج الثابت لجهاز Kiloview E3 NDI Encoder قبل الإصدار 1.30، يتضمن تسع ثغرات قد تتيح السيطرة الكاملة على الجهاز، بتقييم CVSS v3 قدره 9.9.

- المتأثر: البرنامج الثابت لجهاز Kiloview E3 في الإصدارات الأقدم من 1.30.
- تسع ثغرات مسجلة، من CVE-2026-109122 إلى CVE-2026-110825.
- تشمل أنواع الضعف حقن أوامر نظام التشغيل، وغياب المصادقة لوظيفة حرجة، وعدم كفاية انتهاء الجلسات، والتنقل في المسارات، وإلغاء مرجع مؤشر فارغ، وبيانات اعتماد مضمّنة.
- قد يؤدي الاستغلال الناجح إلى السيطرة الكاملة على الجهاز، وتقييم CVSS v3 هو 9.9.
- تحدد CISA القطاعات المعنية بالاتصالات وتقنية المعلومات، مع انتشار الجهاز حول العالم.

ما الذي نُشر

أصدرت CISA تنبيهاً ضمن أنظمة التحكم الصناعي يخص جهاز Kiloview E3 NDI Encoder. والمنتج المتأثر هو البرنامج الثابت للجهاز في الإصدارات الأقدم من 1.30. ويورد التنبيه تسع ثغرات برقم CVE، وتقييم CVSS v3 من المورّد بلغ 9.9.

تندرج نقاط الضعف في ست فئات: **حقن أوامر نظام التشغيل**، وغياب المصادقة لوظيفة حرجة، وعدم كفاية انتهاء الجلسات، والتنقل في المسارات، وإلغاء مرجع مؤشر فارغ، واستخدام بيانات اعتماد مضمّنة. وبحسب CISA، قد يتيح الاستغلال الناجح للمهاجم السيطرة الكاملة على الجهاز.

ومن الثغرات المدرجة CVE-2026-109122 المتعلقة بخدمة إدارة الشبكة، إذ لا تعالج بصورة سليمة أحد الحقول المستخدمة عند ضبط المسارات الثابتة عبر واجهة الإدارة البرمجية، ما قد يتيح لمستخدم موثّق يملك صلاحية ضبط المسارات تنفيذ أوامر.

لماذا يهم ذلك

تربط CISA المنتج بقطاعي الاتصالات وتقنية المعلومات، وتشير إلى انتشاره عالمياً، ومقر الشركة في الصين. وينبغي للجهات التي تستخدم هذه الأجهزة في البث أو الاجتماعات أو شبكات الفيديو الداخلية التحقق من وجود أي وحدات E3 في شبكاتها.

الخطوات المقترحة

ابدأ بحصر أجهزة Kiloview E3 وإصدارات برامجها الثابتة، ثم راجع تنبيه CISA الكامل وإرشادات المورّد لمعرفة الإصدار المصحَّح وأي إجراءات تخفيف إضافية، فالمقتطف المتاح لا يفصّلها. وإلى حين التحديث، قيّد الوصول إلى واجهات إدارة الأجهزة.

ما يجب فعله الآن

1. حصر جميع وحدات Kiloview E3 NDI Encoder وتسجيل إصدارات برامجها الثابتة.
2. التخطيط لتحديث البرنامج الثابت إلى الإصدار 1.30 أو أحدث واختباره، وفق إرشادات المورّد وتنبيه CISA الكامل.
3. حصر الوصول إلى واجهات إدارة الأجهزة في شبكة إدارة مخصصة ولمسؤولين مصرّح لهم فقط.
4. مراجعة الحسابات ذات صلاحية ضبط المسارات وتغيير أي بيانات اعتماد افتراضية أو مشتركة.
5. رصد هذه الأجهزة بحثاً عن تغييرات غير متوقعة في الإعدادات أو اتصالات صادرة غير معتادة.