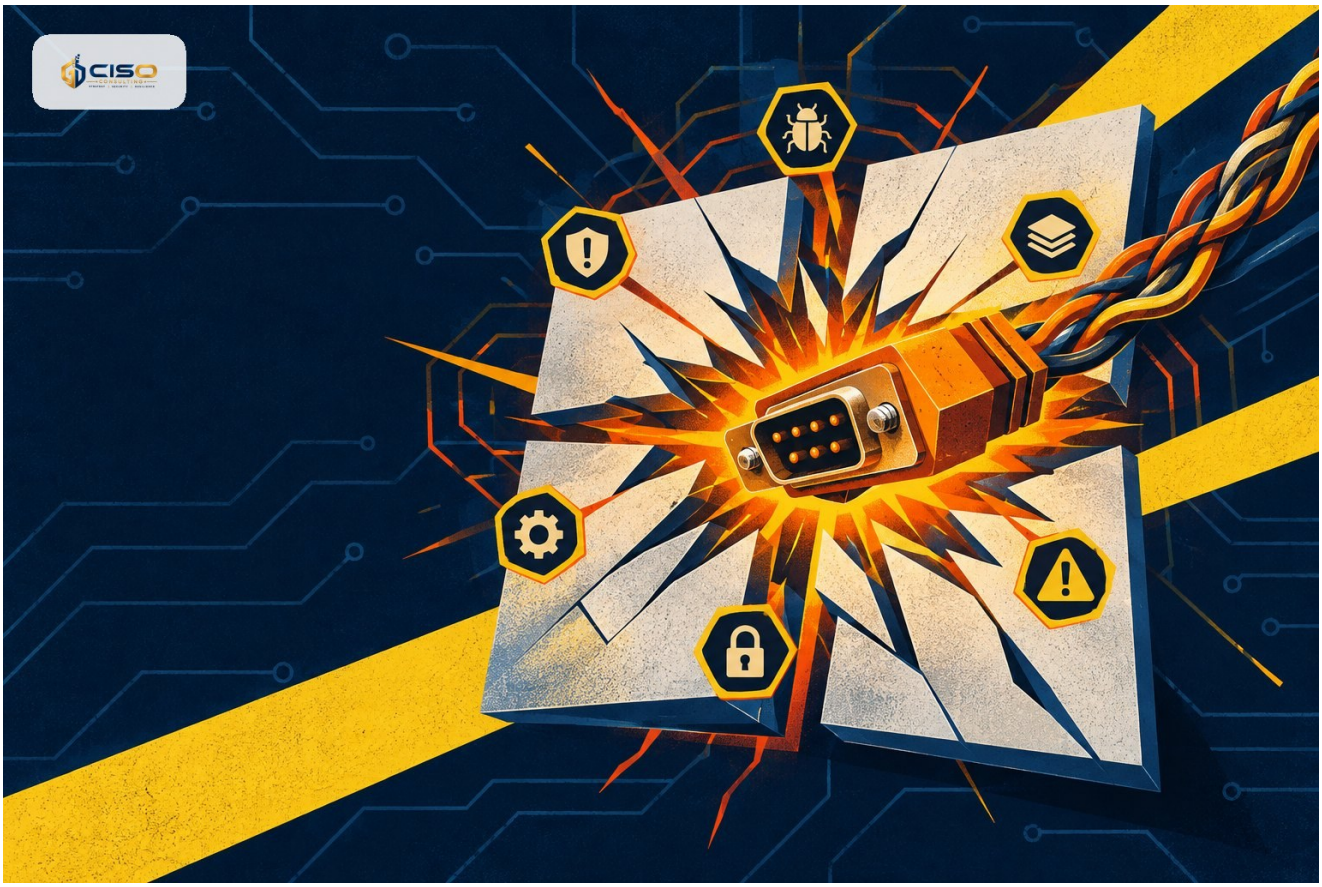
CISA تحذّر من ثغرات تتسبب في تعطل نواة ويندوز في برامج تشغيل PCAN من HMS Networks و-PEAK System



نشرت CISA نشرة عن برامج تشغيل PCAN لنظام ويندوز من HMS Networks وPEAK-System، تشمل ست ثغرات قد يؤدي استغلالها إلى تعطل نواة ويندوز، بتقييم CVSS v3 قدره 7.1.

- قد يؤدي الاستغلال الناجح إلى تعطل نواة ويندوز.
- الإصدارات المتأثرة: PEAK-System Device Driver Setup حتى 5.1.2.1151، وبرامج تشغيل PCAN Windows CAN device drivers حتى 5.1.2.
- ست ثغرات مدرجة: CVE-2026-109576 وCVE-2026-101103 وCVE-2026-94188 وCVE-2026-103672 وCVE-2026-110322 وCVE-2026-105960.
- تشمل أنواع الضعف: الكتابة خارج الحدود، وفيض المخزن المؤقت، وضعف التحقق من فهرس المصفوفة، والإشارة إلى مؤشر غير موثوق، وعدم اتساق معامل الطول.

- تذكر CISA قطاعات منها النقل والرعاية الصحية والطاقة والتصنيع الحيوي، ومقر الشركة في السويد.

نشرت CISA نشرة خاصة بأنظمة التحكم الصناعي تتناول برامج تشغيل PCAN من PEAK-System لنظام ويندوز، والمرتبطة بشركة HMS Networks. وتفيد النشرة بأن الاستغلال الناجح للثغرات المذكورة قد يؤدي إلى تعطل نواة ويندوز.

ما المتأثر

تحدد النشرة مكونين: PEAK-System Device Driver Setup في الإصدارات حتى 5.1.2.1151 ضمناً، وبرامج PCAN Windows CAN device drivers في الإصدارات حتى 5.1.2 ضمناً. ويرتبط المكونان بالثغرات الست نفسها: CVE-2026-109576 وCVE-2026-101103 وCVE-2026-94188 وCVE-2026-103672 وCVE-2026-110322 وCVE-2026-105960.

وتشمل أنواع الضعف الكتابة خارج الحدود، وفيض المخزن المؤقت، وضعف التحقق من فهرس المصفوفة، والإشارة إلى مؤشر غير موثوق، وعدم اتساق معامل الطول. ويبلغ تقييم CVSS v3 لمعدات المورّد 7.1. ويصف أول إدراج محلّلًا اكتشف سجلًا مشوّهاً لكنه واصل زيادة عدّاد البايتات المعالجة.

أهمية الأمر

تذكر CISA قطاعات النقل والرعاية الصحية والصحة العامة والطاقة والتصنيع الحيوي، مع انتشار عالمي. وقد يعطّل تعطل النواة في جهاز ويندوز المتصل بأجهزة CAN أعمال الهندسة أو الاختبار أو المراقبة. ولا يذكر المقتطف الذي راجعناه إصداراً مُصحَّحاً أو إجراءات تخفيف، لذا ينبغي الرجوع إلى نشرة CISA الكاملة وإرشادات المورّد قبل اتخاذ الإجراء.

ما يجب فعله الآن

1. حصر أجهزة ويندوز التي عليها PEAK-System Device Driver Setup أو برامج تشغيل PCAN وتسجيل إصداراتها.
2. مقارنة الإصدارات بالنطاقات المتأثرة: حتى 5.1.2.1151 لحزمة الإعداد وحتى 5.1.2 لبرامج التشغيل.
3. مراجعة نشرة CISA الكاملة وإرشادات HMS Networks أو PEAK-System لمعرفة الإصدارات المُصحَّحة وإجراءات التخفيف.
4. حصر الوصول إلى محطات العمل المتأثرة على المستخدمين المصرّح لهم وتجنب تعريضها لشبكات غير موثوقة.
5. إدراج هذه الأجهزة ضمن متابعة التحديثات لأنظمة التقنية التشغيلية ونقاط النهاية في إطار الحوكمة.