سيمنز PSS SINCAL: ثغرة في مشغّل WibuKey قد تُسبب تعطّل الأنظمة التي تستخدم ترخيص الدونغل



أصدرت CISA تنبيهًا عن ثغرة كتابة خارج الحدود (CVE-2026-84854) في مكوّن WibuKey ضمن PSS SINCAL من سيمنز قد تؤدي إلى حجب الخدمة، وتقتصر على التثبيتات التي تستخدم ترخيص الدونغل القديم.

- الثغرة CVE-2026-84854 هي كتابة خارج الحدود في مشغّل WibuKey التابع لجهة خارجية.
- قد يؤدي استغلالها إلى تعطّل النظام وحجب الخدمة.
- التأثير مقتصر على PSS SINCAL المضبوط على نوع ترخيص دونغل WibuKey القديم.
- الإصدارات المتأثرة: V21.5 وV22.0 (جميع الإصدارات) وV22.5 قبل 22.5.5.
- تعمل سيمنز على إعداد تحديثات وتوصي بإجراءات تخفيف حيث لا تتوفر الإصلاحات بعد.

نشرت CISA تنبيهًا بشأن برنامج PSS SINCAL من سيمنز يتعلق بثغرة في WibuKey، وهو مكوّن من جهة خارجية يستخدمه البرنامج في الترخيص.

ما الذي تأثر

الثغرة المسجّلة برقم **CVE-2026-84854** موجودة في مشغّل WibuKey، حيث يؤدي ضعف التحقق من مدخلات المستخدم عند حساب حجم مخزن مؤقت في النواة إلى كتابة بيانات خارج الحدود. وقد يتسبب استغلالها في تعطّل النظام وبالتالي حجب الخدمة.

لا تهمّ المسألة إلا عند ضبط PSS SINCAL على استخدام نوع ترخيص الدونغل القديم WibuKey. والإصدارات المتأثرة هي V21.5 وV22.0 (جميع الإصدارات) وV22.5 قبل 22.5.5.

تذكر CISA أن القطاعات المعنية تشمل الطاقة والنقل والخدمات المالية والرعاية الصحية والخدمات الحكومية والتصنيع الحرج، مع انتشار عالمي، ومقر سيمنز في ألمانيا.

حالة الإصلاحات

تعمل سيمنز على إعداد تحديثات وتوصي بإجراءات تخفيف للمنتجات التي لم تتوفر لها إصلاحات بعد. ولا يفضّل المصدر المتاح هذه الإجراءات، لذا ينبغي الرجوع إلى تنبيهي سيمنز وCISA مباشرة.

الخطوات المقترحة

على الجهات التي تستخدم PSS SINCAL في تخطيط الشبكات وتحليلها أن تحدد أولاً ما إذا كانت أي تثبيتات تعتمد ترخيص الدونغل القديم. فإن لم يكن ذلك قائمًا فلا ينطبق عليها التعرض المذكور. وإن كان قائمًا فينبغي التخطيط للانتقال إلى إصدار مصحَّح وتطبيق توجيهات سيمنز المؤقتة في الأثناء.

ما يجب فعله الآن

1. حصر جميع تثبيتات PSS SINCAL وتوثيق الإصدار ونوع الترخيص.
2. تحديد التثبيتات التي تستخدم ترخيص الدونغل القديم WibuKey لأنها وحدها المتأثرة.
3. ترقية تثبيتات V22.5 إلى 22.5.5 أو أحدث، والتخطيط لترقية V21.5 وV22.0 عند صدور تحديثات سيمنز.
4. تطبيق إجراءات التخفيف التي توصي بها سيمنز حيث لا يتوفر إصلاح بعد.
5. حصر الوصول إلى محطات العمل التي تشغّل التثبيتات المتأثرة على المستخدمين المصرّح لهم.
6. متابعة تنبيه سيمنز لمعرفة صدور التحديثات وتوثيق القرارات في سجل المخاطر.