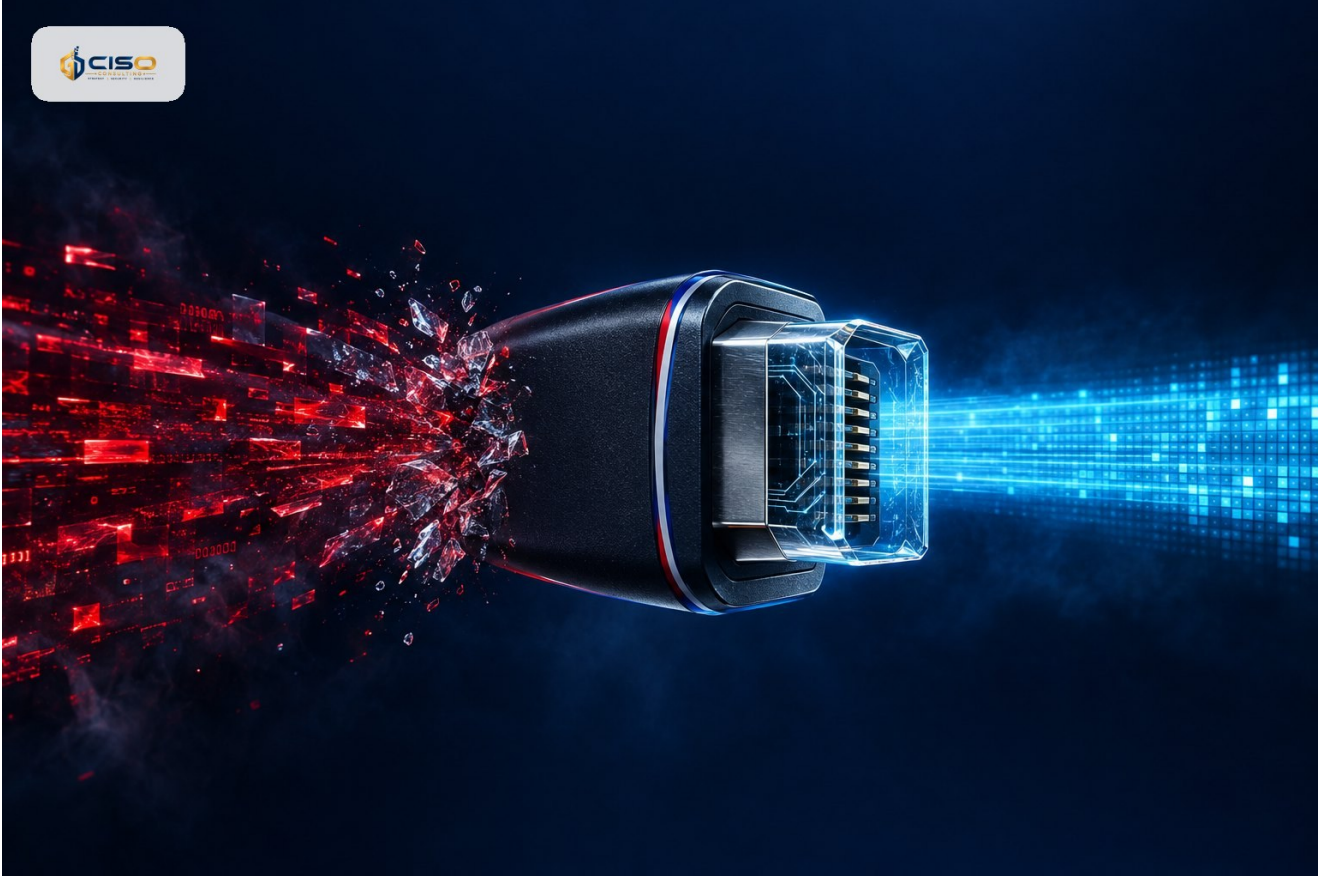


جهاز SilentGlass من المركز الوطني للأمن السيبراني البريطاني يوجب اتصالات HDMI و DisplayPort الخبيثة



رخص المركز الوطني للأمن السيبراني البريطاني لشركة Goldilock Labs تسويق SilentGlass، وهو جهاز يوجب أي اتصال غير متوقع أو خبيث بين الحواسيب والشاشات، ويعامل منافذ العرض كحدّ أمني.

- SilentGlass جهاز يُوصّل مباشرة دون إعداد معقد، ويوجب أي نشاط غير متوقع أو خبيث عبر وصلات HDMI و DisplayPort نحو الشاشات.
- ابتكر المركز الوطني للأمن السيبراني البريطاني الملكية الفكرية للجهاز ورخص لشركة Goldilock Labs بيعه عالمياً بالشراكة مع Sony UK Technology Centre.
- الجهاز منتشر بالفعل في مرافق الحكومة البريطانية ومعتمد للاستخدام في البيئات عالية التهديد.
- يقدر المركز أن الشاشات وسيلة مرّجحة جدّاً للوصول إلى الشبكات بغرض التجسس أو التعطيل أو الكسب المالي.

- من مصادر الخطر المذكورة سلاسل الإمداد وصيانة الأطراف الثالثة والوصول المادي المباشر.

أعلن المركز الوطني للأمن السيبراني البريطاني (NCSC) عن جهاز SilentGlass، وهو يُوضَع بين الحاسوب والشاشة ويحجب أي نشاط غير متوقع أو خبيث عبر وصلات HDMI و DisplayPort. وقد ابتكر المركز الملكية الفكرية للجهاز، ورخص لشركة Goldilock Labs تصنيعه وبيعه عالميًا بالشراكة مع Sony UK Technology Centre.

لماذا تهتم وصلات العرض

يرى المركز أن الشاشات هدف جذاب لأنها قد تحمل بيانات حساسة أو شخصية وتعالجها. ويعدّ استخدامها للوصول إلى الشبكات بغرض التجسس أو التعطيل أو الكسب المالي أمرًا مرجّحًا جدًّا، مشيرًا إلى أن إجراءات المعالجة المتاحة غالبًا ما تكون مكلفة وغير فعّالة.

ويرى المركز أن واجهات العتاد نادرًا ما عوملت كحدود أمنية، رغم تعرضها للمخاطر عبر سلاسل الإمداد وصيانة الأطراف الثالثة والوصول المادي المباشر.

ما الذي يقدّمه المنتج

يعمل SilentGlass بمجرد توصيله، وقد استُخدم فعلاً في مرافق الحكومة البريطانية. ويذكر المركز أنه معتمد للاستخدام في أشد البيئات تهديدًا، وأنه متاح الآن لأي مشترٍ، ومنهم قطاعات البنية التحتية الوطنية الحرجة والشركات. ويقدمه المركز بوصفه خطوة أولى نحو ضبط السلوك عند واجهات العتاد قبل وصوله إلى البرمجيات المعقدة.

قراءة عملية

لا يذكر المصدر مواصفات تقنية ولا أسعارًا ولا نتائج اختبار مستقلة، لذا ينبغي التعامل مع الخبر كإشارة إلى طبيعة الخطر لا كتركيبة لمنتج. والرسالة الأوسع أن الاتصال المادي يجب أن يكون نقطة تحكم لا حدّ ثقة مفترضًا.

ما يجب فعله الآن

1. أدرجوا منافذ العرض والملحقات (HDMI و DisplayPort) ضمن نماذج التهديد الخاصة بالوصول المادي والأجهزة الطرفية.
2. راجعوا المناطق عالية الحساسية، مثل قاعات التداول ومراكز العمليات الأمنية ومكاتب الإدارة العليا، ومدى اعتمادها على شاشات أو محطات توصيل مشتركة أو تخضع لصيانة أطراف ثالثة.
3. اشترطوا الإشراف والتسجيل عند قيام أطراف ثالثة بصيانة أجهزة العرض أو استبدالها.
4. اطلبوا من الموردين أدلة اختبار مستقلة قبل تقييم أي منتج لحجب منافذ العتاد، بما في ذلك SilentGlass.
5. اربطوا النتائج بضوابط الأمن المادي وإدارة مخاطر الأطراف الثالثة في الضوابط الأساسية للأمن السيبراني (ECC) وإطار الأمن السيبراني لمؤسسة النقد (SAMA CSF).