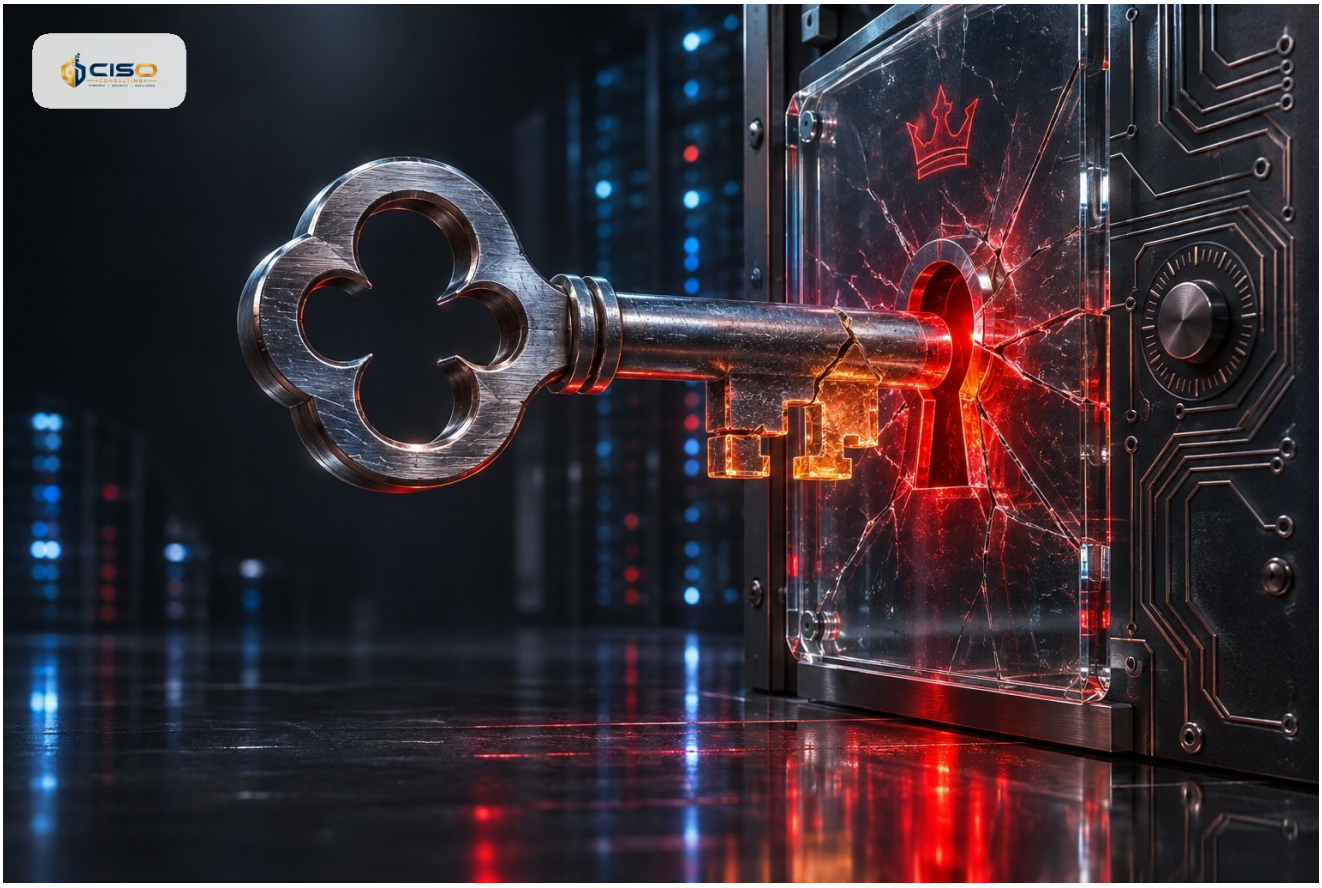
ASUS تصدر تحديثًا لثغرات حرجة في مفاتيح مضمّنة بمنتج Control Center Express



أصدرت ASUS النسخة v1.7.29 من Control Center Express لمعالجة ثلاث ثغرات حرجة، منها (CVSS 10.0) CVE-2026-114202 التي تتيح لمهاجم عن بُعد دون مصادقة انتحال رمز دخول والحصول على صلاحيات المسؤول.

- تم إصلاح ثلاث ثغرات حرجة في Control Center Express v1.7.29: CVE-2026-114202 وCVE-2026-114204 وCVE-2026-114205.
- الثغرة (CVSS 10.0) CVE-2026-114202 ناتجة عن مفتاح تشفير مضمّن ولا تتطلب صلاحيات أو تفاعل مستخدم.
- الثغرة CVE-2026-114204 تتيح انتحال رمز جلسة لحساب سجّل دخوله حديثًا، وCVE-2026-114205 تتيح لمستخدم محدود الصلاحيات إنشاء حساب مسؤول.
- تذكر ASUS أن النسخ السابقة لـ v1.7.29 متأثرة، بينما تسرد سجلات CVE النسخ حتى v1.7.27

فقط، فوضع v1.7.28 غير واضح.

- شملت التحديثات أيضًا Armoury Crate، Control Center Datacenter، Control Center Enterprise ومنها الثغرة الحرجة CVE-2026-126574.

أصدرت ASUS النسخة v1.7.29 من Control Center Express لمعالجة ثلاث ثغرات حرجة قد تتيح لمهاجمين عن بُعد السيطرة الإدارية على لوحة الإدارة والأجهزة التي تديرها.

ما الذي تم إصلاحه

أخطرها CVE-2026-114202 بدرجة CVSS 10.0، وسببها مفتاح تشفير مضمّن في المنتج، وتتيح لمهاجم عن بُعد دون مصادقة انتحال رمز مصادقة والحصول على صلاحيات المسؤول دون أي تفاعل من المستخدم.

أما CVE-2026-114204 فهي كذلك مشكلة مفتاح مضمّن، وتسمح لمهاجم محدود الصلاحيات بانتحال رمز جلسة لحساب سجّل دخوله حديثًا. وتتعلق CVE-2026-114205 بخلل في التفويض يتيح لمستخدم محدود الصلاحيات إنشاء حساب مسؤول.

يُستخدم Control Center Express لوحةً مركزية لدى مسؤولي تقنية المعلومات لمراقبة أجهزة الحاسب وإدارتها عن بُعد، وتسوّقه ASUS للشركات ومزوّدي خدمات تقنية المعلومات.

النطاق وعدم وضوح النسخ

تفيد نشرة ASUS بأن النسخ الأقدم من v1.7.29 متأثرة، في حين تذكر سجلات CVE النسخ المتأثرة حتى v1.7.27 فقط، ما يجعل وضع v1.7.28 غير واضح. والأحوط التعامل معها على أنها متأثرة.

تحديثات أخرى من ASUS

عالجت ASUS أيضًا CVE-2026-126574، وهي ثغرة حرجة تتيح لمستخدم بدور Viewer محدود الصلاحيات تغيير كلمة مرور مسؤول، وتشمل Control Center Datacenter حتى 4.0.0.2 وControl Center Enterprise حتى 3.1.0.8. كما حُدّث Armoury Crate لمعالجة CVE-2026-112115، وهي ثغرة رفع صلاحيات محلية عالية الخطورة تشمل النسخ حتى 6.7.2 ضمنًا.

لا يشير المصدر إلى استغلال فعلي للثغرات.

ما يجب فعله الآن

1. حصر أماكن تشغيل ASUS Control Center Express وControl Center Enterprise وControl Center Datacenter وArmoury Crate.
2. ترقية Control Center Express إلى v1.7.29 بما في ذلك تثبيتات v1.7.28، ثم تحديث الوكلاء على الأجهزة المُدارة عبر Client Agent Updater ← Select Function والتحقق من النسخ.
3. تطبيق تحديثات المورّد لكل من Armoury Crate، Control Center Datacenter، Control Center Enterprise.
4. إلى حين التحديث، تقييد الوصول الشبكي إلى لوحة الإدارة بشبكات المسؤولين الموثوقة.

5. مراجعة حسابات المسؤولين وتغييرات كلمات المرور الأخيرة في هذه المنصات بحثًا عن إنشاء أو تعديل غير متوقع.
6. توثيق المعالجة ضمن إدارة الثغرات والتحديثات لأغراض أدلة ضوابط الهيئة الوطنية للأمن السيبراني (ECC) وإطار الأمن السيبراني للبنك المركزي السعودي (SAMA CSF).