أجهزة Siemens SIMATIC IPC: مفتاح اختبار يُضعف UEFI Secure Boot (CVE-2026-72895)



أفادت CISA بأن مفتاح اختبار من مورّد BIOS في قاعدة بيانات UEFI Secure Boot لعدة أجهزة Siemens SIMATIC IPC قد يتيح لمهاجم محلي تجاوز الحماية. وأصدرت Siemens إصدارات مصححة وتوصي بالتحديث.

- الثغرة CVE-2026-72895 تتعلق باستخدام مفتاح تشفير افتراضي: يوجد مفتاح اختبار من مورّد BIOS في قاعدة مفاتيح Secure Boot.
- يمكن لمهاجم محلي يملك وصولًا فعلياً أو إدارياً تشغيل نظام تشغيل أو تطبيق UEFI موقّع بهذا المفتاح حتى مع تفعيل Secure Boot.
- الإصدارات المتأثرة: SIMATIC IPC BX-21A دون 31.01.13، وIPC RW-543A دون 1.1.4، وIPC227G/277G/277G PRO/327G/377G دون 28.01.15.
- درجة CVSS v3 تبلغ 7.7.

- أصدرت Siemens إصدارات جديدة وتوصي بالتحديث إلى أحدثها.

ما الذي ورد في النشرة

نشرت CISA تنبيهاً بشأن عدة أجهزة حاسب صناعية من Siemens ضمن عائلة SIMATIC. يوجد مفتاح اختبار من موزّد BIOS داخل قاعدة مفاتيح UEFI Secure Boot (الثغرة CVE-2026-72895، وتصنَّف استخداماً لمفتاح تشفير افتراضي)، وتبلغ درجة CVSS v3 نحو 7.7.

يستطيع مهاجم محلي يملك وصولًا فعلياً أو إدارياً إلى الجهاز استغلال المفتاح لتشغيل نظام تشغيل أو تطبيق UEFI موقّع به، وبذلك يتجاوز حماية UEFI Secure Boot حتى لو كانت مفعّلة.

المنتجات المتأثرة

- SIMATIC IPC BX-21A: الإصدارات الأقل من 31.01.13
- SIMATIC IPC RW-543A: الإصدارات الأقل من 1.1.4
- SIMATIC IPC227G وIPC277G وIPC277G PRO وIPC327G وIPC377G: الإصدارات الأقل من 28.01.15

وتشير CISA إلى أن القطاعات المعنية تشمل التصنيع الحرج والنقل والطاقة والصحة والخدمات المالية والمرافق الحكومية، مع انتشار الأجهزة عالمياً.

الخطوات المقترحة

أصدرت Siemens إصدارات جديدة للمنتجات المتأثرة وتوصي بالتحديث إلى أحدثها. ولأن الاستغلال يتطلب وصولًا محلياً فعلياً أو إدارياً، ينبغي أولًا حصر أماكن تركيب هذه الأجهزة ثم جدولة التحديث عبر إجراءات إدارة التغيير المعتادة. ولا تذكر النشرة رصد استغلال فعلي للثغرة.

ما يجب فعله الآن

1. حصر أجهزة SIMATIC IPC BX-21A وRW-543A وIPC227G/277G/277G PRO/327G/377G وتسجيل إصدارات BIOS الحالية.
2. جدولة التحديث إلى الإصدارات المصححة من Siemens عبر إدارة التغيير مع اختبار مناسب للبيئات التشغيلية.
3. تقييد الوصول الفعلي إلى الأجهزة المتأثرة ومراجعة من يملك صلاحيات إدارية عليها.
4. عند تعذر التحديث الفوري، توثيق الاستثناء والضوابط البديلة في سجل المخاطر.
5. التحقق بعد التحديث من أن الأجهزة تعمل بالإصدارات المصححة.