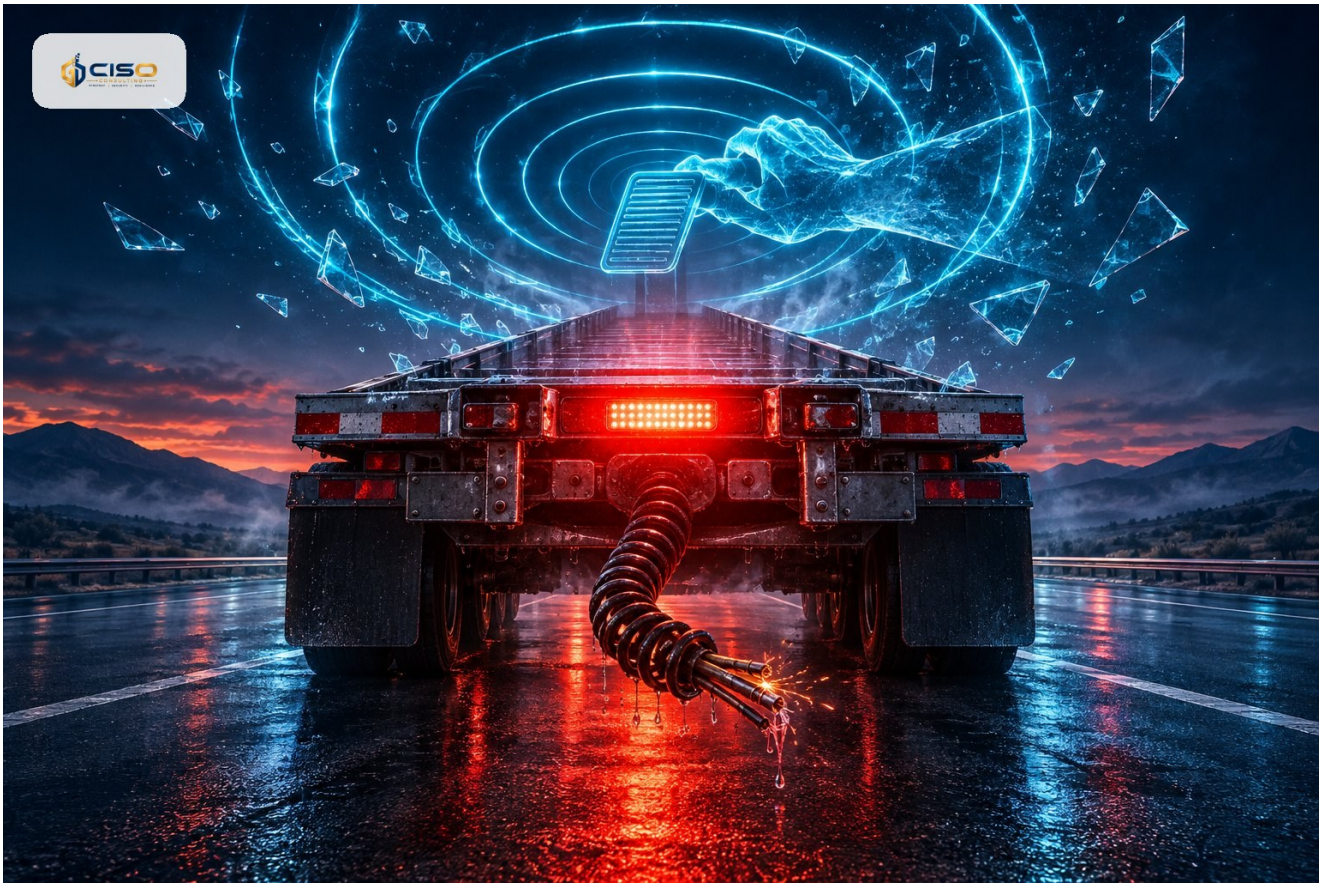
ثغرات Bluetooth في وحدات Elecbrakes تتيح لمهاجم قريب التحكم في فرامل المقطورات



كشف باحثون ثغرات Bluetooth في وحدات فرامل المقطورات من Elecbrakes تتيح لمهاجم دون مصادقة وضمن النطاق تفعيل الفرامل أو تحريرها. صدرت تحديثات لـ EB2 وVM1، بينما ما زال الإصلاح لـ ELBC 2000 قيد الإعداد.

- المنتجات المتأثرة هي وحدات EB2 وVM1 وELBC 2000، وتُستخدم بصورة رئيسية في أستراليا ونيوزيلندا بحسب CISA.
- ثغرتان حرجتان (غياب المصادقة وضعف الحماية من إعادة الإرسال) تتيحان لمهاجم ضمن نحو 100 متر تفعيل الفرامل أو تحريرها أو تعديل قوتها دون أي تفاعل من الضحية.
- ثغرة ثالثة متوسطة الخطورة في آلية تحديث البرنامج الثابت قد تتيح نظريًا اختراقًا دائمًا، ولم يثبت الباحثون ذلك عمليًا.
- صدرت تحديثات البرنامج الثابت في أوائل يوليو لوحدتي EB2 وVM1، وخطة المعالجة لـ ELBC 2000

ما زالت قيد الإعداد.

- لا توجد أدلة على استغلال خبيث للثغرات.

كشف باحثون من شركة Element Digital الأسترالية للاستشارات التقنية والأمن السيبراني ثلاث ثغرات في وحدات التحكم بفرامل المقطورات العاملة عبر Bluetooth من إنتاج Elecbrakes. ونشرت CISA إشعارًا بشأنها، مشيرة إلى أن هذه المنتجات تُستخدم أساسًا في أستراليا ونيوزيلندا.

ما الذي اكتُشف

النماذج المتأثرة هي EB2 (تُركَّب على المقطورة) وVM1 (تُركَّب على المركبة القاطرة) وELBC 2000 الأقدم. تضبط هذه الوحدات قوة الفرملة المطبقة على المقطورة، ويمكن تشغيلها عبر جهاز تحكم مخصص أو تطبيق على الهاتف.

ثغرتان مصنفتان حرجتين: غياب المصادقة، وعدم كفاية الحماية من هجمات إعادة الإرسال. وأظهر الباحثون أن مهاجمًا غير مصادَق ضمن نطاق Bluetooth، حتى 100 متر، يستطيع باستخدام حاسوب محمول أو هاتف تفعيل الفرامل أو تحريرها أو تغيير قوتها دون أي تدخل من الضحية. أما الثغرة الثالثة فمتوسطة الخطورة وتتعلق بآلية تحديث البرنامج الثابت، وقد تتيح نظريًا اختراقًا دائمًا، لكن الباحثين لم يحاولوا تثبيت برنامج خبيث.

حالة الإصلاحات

أُبلغت Elecbrakes في منتصف مايو، وأصدرت برنامجًا ثابتًا مصححًا لوحدتي EB2 وVM1 في أوائل يوليو. وبعد التحديث يتطلب الوصول عن بُعد اقترانًا أوليًا يستلزم وصولاً ماديًا إلى الجهاز ولا يمكن إجراؤه عبر Bluetooth. أما ELBC 2000 فخطة المعالجة ما زالت قيد الإعداد، وتنصح الشركة المالكين بإبقاء اتصال نشط بين الوحدة وهاتفهم أو جهاز التحكم أثناء الاستخدام. وذكرت الشركة لموقع iTnews أنها نبّهت نحو 40 ألف مستخدم للتطبيق وأن التحديث ثُبّت على 60-70% من الوحدات التي تتصل يوميًا. ولم يُبلَّغ عن استغلال خبيث.

الأهمية

تبيّن الحالة أن ميزات الاتصال اللاسلكي قصير المدى في المعدات التشغيلية قد تنشئ مخاطر على السلامة المادية عند ضعف المصادقة. وعلى الجهات التي تشغّل أساطيل مركبات أو معدات بمكونات مشابهة التحقق من تعرضها.

ما يجب فعله الآن

1. التحقق من استخدام أي مقطورات أو معدات أسطول لوحدات Elecbrakes من طراز EB2 أو VM1 أو ELBC 2000، بما فيها ما يوفره المقاولون.
2. تطبيق تحديث البرنامج الثابت من المورّد على وحدات EB2 وVM1 وتوثيق إتمامه في سجل الأصول.
3. بالنسبة لوحدات ELBC 2000، اتباع إرشادات المورّد المؤقتة بإبقاء الوحدة متصلة اتصالاً نشطًا بالهاتف أو جهاز التحكم أثناء الاستخدام، ومتابعة خطة المعالجة المرتقبة.
4. إدراج المعدات التشغيلية والمركبات التي تعمل بـ Bluetooth في سجلات الأصول وتقييمات المخاطر، مع مراجعة آليات المصادقة والتحديث.

5. الاستفسار من موردي المعدات المتصلة عن سياساتهم في الإفصاح عن الثغرات وإصدار التصحيحات.