

تحذير من وكالة الأمن السيبراني الأمريكي بشأن ثغرات المصادقة وبيانات الاعتماد في مفاتيح Red Lion N-Tron 700 الصناعية



أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً بشأن سبع ثغرات في مفاتيح Red Lion Controls N-Tron 700 الصناعية قد تتيح وصولاً إدارياً غير مصرح به وإعادة تشغيل الأجهزة عن بُعد.

- سبع ثغرات تؤثر على مفاتيح Red Lion N-Tron 700 التي تعمل بإصدار البرنامج الثابت 3.11.0 أو أقدم وإصدار محمل الإقلاع 2.0.6.1 أو أقدم
- تشمل الثغرات بيانات اعتماد مشفرة مسبقاً وحماية غير كافية لبيانات الاعتماد وغياب المصادقة وآليات تجاوز المصادقة
- يمنح الاستغلال الناجح وصولاً إدارياً لعرض وتعديل وتحميل ملفات التكوين
- يمكن للمهاجمين إجبار الأجهزة على إعادة التشغيل المستمر عبر الانتقال إلى عنوان URL محدد

يمكن أتمتته بواسطة برنامج نصي

- درجة CVSS البالغة 8.3 تشير إلى خطورة عالية في بيانات البنية التحتية الحرجة

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً خاصاً بأنظمة التحكم الصناعي بشأن ثغرات متعددة تؤثر على مفاتيح Ethernet الصناعية المُدارة من طراز Red Lion Controls N-Tron 700. تحمل الثغرات درجة CVSS مجمعة قدرها 8.3 وتؤثر على الأجهزة التي تعمل بإصدار البرنامج الثابت 3.11.0 أو أقدم وإصدار محمل الإقلاع 2.0.6.1 أو أقدم.

طبيعة الثغرات

يحدد التنبيه سبعة إدخلالات CVE متميزة تشمل نقاط ضعف في المصادقة وإدارة بيانات الاعتماد. تشمل الثغرات بيانات اعتماد مشفرة مسبقاً، وحماية غير كافية لبيانات الاعتماد، وكلمات مرور مخزنة بصيغة قابلة للاسترداد، وغياب المصادقة للوظائف الحرجة، وتنزيل التعليمات البرمجية دون فحص السلامة، وثغرات تأكيد قابلة للوصول، وتجاوز المصادقة عبر مسارات بديلة. يتيح الاستغلال الناجح لجهة خبيثة الحصول على وصول إداري كامل للجهاز، مما يسمح بعرض وتعديل وتحميل ملفات التكوين.

مخاطر حجب الخدمة

بالإضافة إلى الوصول غير المصرح به، تتيح الثغرات للمهاجم تشغيل وإعادة تشغيل الجهاز عبر الانتقال إلى عنوان URL محدد على المفتاح. يمكن برمجة هذا الإجراء وأتمتته على جهاز المهاجم المحلي للتسبب في إعادة تشغيل مستمرة، مما يخلق فعلياً حالة حجب خدمة تعطل عمليات الشبكة في البيئات الصناعية.

التداعيات على البيانات الخاضعة للتنظيم

بالنسبة للمؤسسات التي تدير البنية التحتية الحرجة أو أنظمة التحكم الصناعي في المملكة العربية السعودية، تمثل هذه الثغرات مخاطر على استمرارية العمليات وسلامتها. تُنشر المفاتيح المتأثرة عادةً في بيانات التصنيع والمرافق وغيرها من بيانات تقنية العمليات حيث تعد توافر الشبكة وسلامة التكوين ضروريين للسلامة والالتزامات التنظيمية.

ما يجب فعله الآن

1. تحديد جميع مفاتيح Red Lion N-Tron 700 في شبكات تقنية العمليات وأنظمة التحكم الصناعي عبر مؤسستك
2. فحص إصدارات البرنامج الثابت ومحمل الإقلاع على الأجهزة المحددة؛ إعطاء الأولوية لتلك التي تعمل بالبرنامج الثابت 3.11.0 أو أقدم ومحمل الإقلاع 2.0.6.1 أو أقدم
3. الاتصال بشركة Red Lion Controls أو الموزع المعتمد للاستفسار عن توفر التحديثات الأمنية وإرشادات الترقية
4. تطبيق تجزئة الشبكة لعزل المفاتيح المتأثرة عن الشبكات غير الموثوقة وتقييد الوصول الإداري للموظفين المصرح لهم فقط
5. مراقبة سجلات الأجهزة وحركة مرور الشبكة لاكتشاف محاولات الوصول الإداري غير المعتادة أو أحداث إعادة التشغيل المتكررة

6. مراجعة وتحديث إجراءات الاستجابة للحوادث لمعالجة سيناريوهات حجب الخدمة المحتملة التي تؤثر على البنية التحتية للشبكات الصناعية