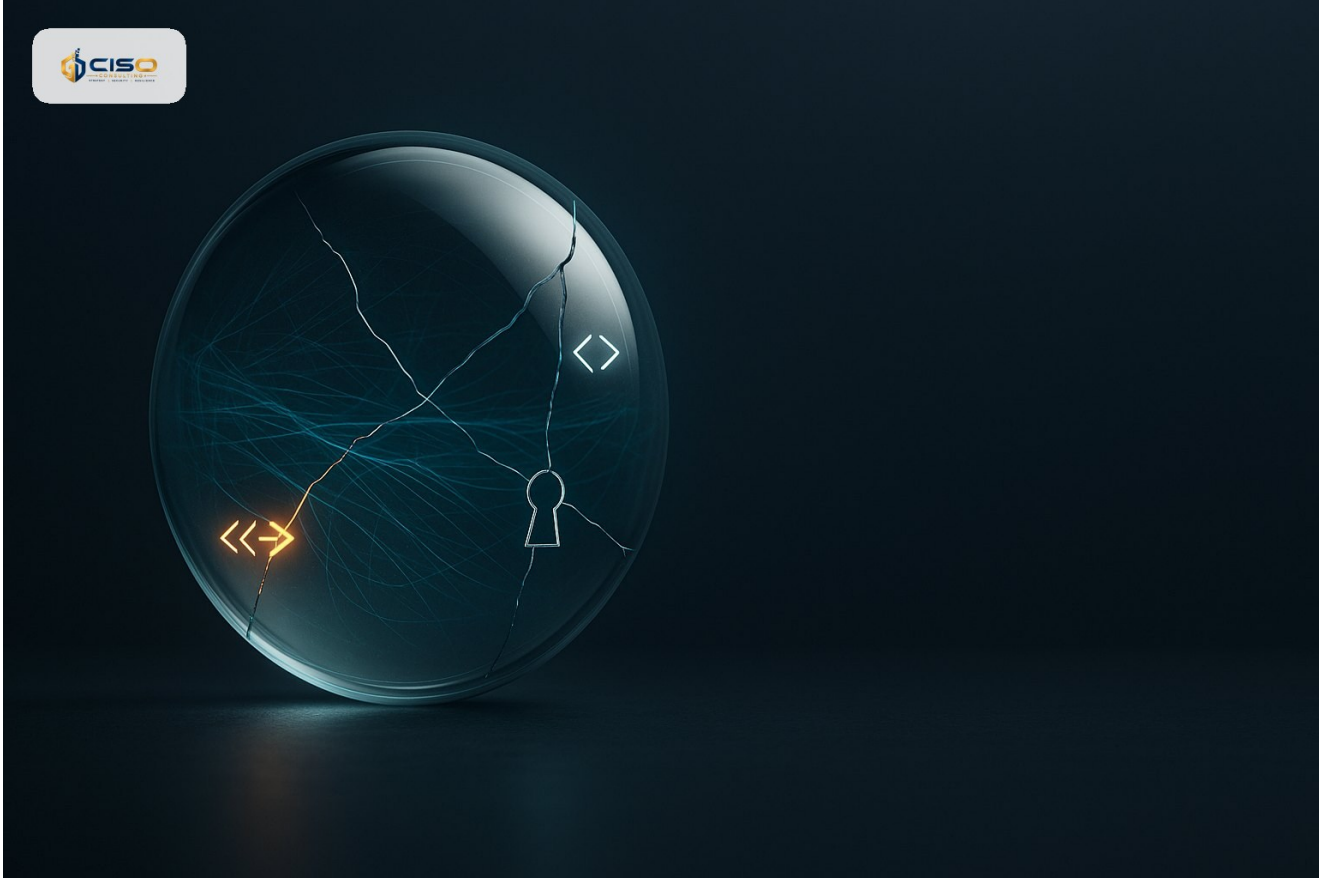


وكالة الأمن السيبراني الأمريكية تصدر تنبيهاً بشأن ثغرات متعددة في منصة Malcolm لتحليل الشبكات



أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً يوضح ثغرات أمنية متعددة في منصة Malcolm لتحليل حركة مرور الشبكات، تشمل ثغرات البرمجة النصية عبر المواقع وحقق الأوامر وتجاوز المصادقة.

- منصة CISA Malcolm لتحليل الشبكات تحتوي على ثغرات أمنية متعددة بدرجة خطورة 8.8 حسب مقياس CVSS
- الثغرات المكتشفة تشمل البرمجة النصية عبر المواقع وحقق أوامر نظام التشغيل واجتياز المسارات والتزوير من جانب الخادم
- ثغرات إضافية تتعلق بتجاوز المصادقة وغياب التفويض واستخدام بيانات اعتماد افتراضية والتحقق غير السليم من الشهادات
- المنصة منتشرة عالمياً وتؤثر على قطاعات البنية التحتية الحرجة بما في ذلك الطاقة وتقنية

ثغرات متعددة تم تحديدها

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً لأنظمة التحكم الصناعي يوضح ثغرات أمنية متعددة في منصة **CISA Malcolm**، وهي منصة لتحليل حركة مرور الشبكات. تحمل الثغرات درجة خطورة مجمعة 8.8 حسب مقياس CVSS v3، مما يشير إلى خطورة عالية. تشمل نقاط الضعف مجموعة واسعة من الثغرات الأمنية بما في ذلك المعالجة غير السليمة للمدخلات التي تؤدي إلى البرمجة النصية عبر المواقع وحقق أوامر نظام التشغيل وهجمات اجتياز المسارات.

تشمل الثغرات الإضافية التزوير من جانب الخادم وتجاوز المصادقة عبر الانتحال وغياب ضوابط التفويض وغياب المصادقة للوظائف الحرجة. يحدد التنبيه أيضاً مشكلات تتعلق بالتفويض غير الصحيح واستخدام بيانات اعتماد افتراضية والتحقق غير السليم من الشهادات وإعادة توجيه عناوين URL إلى مواقع غير موثوقة والاعتماد على مكونات طرف ثالث معرضة للخطر. من الجدير بالذكر أن الثغرة CVE-2026-90443 تتضمن واجهة ويب تعكس أجزاء من عناوين URL المطلوبة في سياقات برمجية دون ترميز كافٍ ولا تتطلب مصادقة للوصول.

نطاق الانتشار والتأثير

منصة Malcolm منتشرة عالمياً وتؤثر على قطاعات البنية التحتية الحرجة بما في ذلك الطاقة وتقنية المعلومات وأنظمة المياه والصرف الصحي. يجعل استخدام المنصة في بيئات التكنولوجيا التشغيلية ومراقبة البنية التحتية الحرجة هذه الثغرات ذات أهمية خاصة للمؤسسات التي تعتمد على الأداة لرؤية الشبكة والتحليل الأمني.

اعتبارات المخاطر للمؤسسات السعودية

يجب على المؤسسات الخاضعة للتنظيم في المملكة التي تستخدم Malcolm لتحليل الشبكات أو المراقبة الأمنية تقييم تعرضها فوراً. يخلق الجمع بين ثغرات تجاوز المصادقة والانتشار المحتمل للمنصة في بيئات البنية التحتية الحرجة مخاطر مرتفعة للوصول غير المصرح به واختراق الأنظمة.

ما يجب فعله الآن

1. تحديد جميع عمليات نشر CISA Malcolm ضمن البنية التحتية للشبكة وبيئات التكنولوجيا التشغيلية
2. مراجعة سجلات الوصول لنسخ Malcolm للكشف عن أي نشاط مشبوه أو محاولات وصول غير مصرح بها
3. تطبيق تجزئة الشبكة لعزل عمليات نشر Malcolm عن الأنظمة الحرجة حتى يتم تطبيق التصحيحات
4. متابعة تنبيهات CISA للحصول على تصحيحات البائع وإرشادات المعالجة الخاصة بأرقام CVE المحددة
5. تقييم ما إذا كانت Malcolm تُستخدم في أي قدرة لمراقبة البنية التحتية الحرجة وتقييم الحلول البديلة إذا لم يكن التصحيح الفوري ممكناً
6. توثيق استخدام Malcolm والتعرض للثغرات كجزء من سجل المخاطر والإبلاغ إلى لجان الحوكمة ذات الصلة