

ثغرة في نظام إدارة المحتوى Strapi تكشف معلومات حساسة عبر لوحة الإدارة



ثغرة تخزين نصي واضح في نظام إدارة المحتوى Strapi تتيح للمهاجمين الذين يملكون صلاحية الوصول إلى لوحة الإدارة اكتشاف تفاصيل المستخدمين الحساسة عبر مرشحات الاستعلام، مع إمكانية تنفيذ أوامر عن بُعد عند ربطها بثغرة أخرى.

- الثغرة CVE-2023-22894 تؤثر على نظام Strapi وتسمح بكشف معلومات المستخدمين الحساسة عبر مرشحات الاستعلام في لوحة الإدارة
- تقوم الثغرة بتخزين المعلومات الحساسة بنص واضح يمكن للمسؤولين المصادق عليهم الوصول إليه
- يمكن ربطها مع الثغرة CVE-2023-22621 لتنفيذ أوامر عن بُعد
- الإصدارات المتأثرة قد تكون منتهية الدعم أو الخدمة
- يُنصح المؤسسات بإيقاف الاستخدام أو الانتقال إلى إصدارات مدعومة

نظرة عامة على الثغرة

يحتوي نظام Strapi، وهو نظام إدارة محتوى مفتوح المصدر، على **ثغرة تخزين بنص واضح** مسجلة برقم CVE-2023-22894. تتيح هذه الثغرة للمهاجمين الذين حصلوا على صلاحية الوصول إلى لوحة الإدارة اكتشاف تفاصيل المستخدمين الحساسة من خلال وظيفة مرشح الاستعلام في المنصة. تتبع الثغرة من تخزين المعلومات الحساسة بصيغة غير مشفرة، مما يجعلها متاحة للمستخدمين المصادق عليهم الذين يملكون صلاحيات إدارية. تتفاقم المخاطر بإمكانية ربط هذه الثغرة مع الثغرة CVE-2023-22621، والتي قد تمكّن المهاجمين من تحقيق **تنفيذ أوامر عن بُعد** على الأنظمة المتأثرة. يزيد مسار التصعيد هذا بشكل كبير من التأثير المحتمل على المؤسسات التي تشغل نسخ Strapi الضعيفة.

حالة المنتج والمعالجة

قد تكون إصدارات Strapi المتأثرة منتهية الدعم أو الخدمة، مما يعني أن دعم المورّد والتحديثات الأمنية قد لا تكون متاحة بعد الآن. يُنصح المؤسسات التي تستخدم Strapi حالياً بتقييم حالة نشرها والنظر في إيقاف استخدام الإصدارات غير المدعومة. وحيثما كان استمرار التشغيل ضرورياً، ينبغي على المؤسسات الانتقال إلى إصدارات مدعومة عالجت هذه الثغرة.

بالنسبة للجهات الخاضعة للتنظيم في المملكة، تمثل هذه الثغرة قلقاً خاصاً نظراً لحساسية البيانات التي تُدار عادة من خلال أنظمة إدارة المحتوى. يتعارض التخزين بنص واضح للمعلومات الحساسة مع متطلبات حماية البيانات وضوابط خط الأساس الأمني التي تفرض تشفير البيانات الحساسة أثناء التخزين.

سياق المخاطر

رغم أن الثغرة تتطلب صلاحية وصول إدارية موجودة مسبقاً، إلا أنها تمثل خطر **تصعيد صلاحيات** وكشف معلومات كبير. في البيئات التي يعمل فيها عدة مسؤولين بمستويات ثقة متفاوتة، أو حيث قد تُخترق بيانات الاعتماد الإدارية، قد يسهّل كشف تفاصيل المستخدمين الحساسة هجمات إضافية أو انتهاكات للامتثال.

ما يجب فعله الآن

1. تحديد جميع نسخ نظام Strapi المنشورة عبر البنية التحتية للمؤسسة، بما في ذلك بيئات التطوير والاختبار والإنتاج
2. التحقق من إصدار وحالة الدعم لكل نشر من Strapi لتحديد ما إذا كانت الإصدارات المتأثرة منتهية الدعم أو الخدمة
3. إيقاف استخدام إصدارات Strapi غير المدعومة أو الترحيل إلى الإصدارات المدعومة الحالية مع تطبيق التصحيحات الأمنية
4. مراجعة سجلات الوصول الإداري لنسخ Strapi لتحديد أي نشاط مشبوه في مرشحات الاستعلام أو وصول غير مصرح به للمعلومات
5. تطبيق ضوابط وصول ومراقبة إضافية للوحدات الإدارية، مع تقييد الوصول بناءً على مبادئ الحد الأدنى من الصلاحيات
6. تقييم ما إذا كانت أي معلومات حساسة قد تعرضت للكشف وبدء إجراءات الاستجابة للحوادث في حال

الاشتباه بوصول غير مصرح به