

ثغرة حقن التعليمات البرمجية في Microsoft SharePoint تتطلب تطبيق التحديثات الأمنية فوراً



يحتوي Microsoft SharePoint على ثغرة حقن تعليمات برمجية تتيح للمهاجمين المصرح لهم تنفيذ تعليمات برمجية عن بُعد عبر الشبكة، مما يستدعي تطبيق التحديثات الأمنية من المورد فوراً.

- الثغرة CVE-2026-65660 تؤثر على Microsoft SharePoint وتسمح بحقن التعليمات البرمجية من قبل مهاجمين مصرح لهم عبر الشبكة
- تتيح الثغرة تنفيذ تعليمات برمجية عن بُعد مما يشكل خطراً كبيراً على بيئات SharePoint
- يجب على المؤسسات تطبيق الإجراءات التصحيحية من المورد فوراً أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- ينبغي للمؤسسات تقييم مدى تعرض الأصول المتأثرة للإنترنت وترتيب أولويات التحديثات بناءً على المخاطر
- تتطلب بيئات الخدمات السحابية اهتماماً خاصاً بإرشادات التحديثات الأمنية المطبقة

نظرة عامة على الثغرة

يتأثر Microsoft SharePoint بثغرة حقن تعليمات برمجية تحمل الرقم التعريفي CVE-2026-65660. تسمح هذه الثغرة لمهاجم مصرح له بتنفيذ تعليمات برمجية عشوائية عبر اتصال الشبكة، مما يشكل تهديداً خطيراً للمؤسسات التي تعتمد على SharePoint للتعاون وإدارة المستندات. تتطلب الثغرة أن يكون لدى المهاجم صلاحيات وصول مصرح بها، مما يشير إلى إمكانية الاستغلال عبر بيانات اعتماد مخترقة أو تهديدات داخلية.

المخاطر على المؤسسات السعودية

تنتشر بيانات SharePoint على نطاق واسع في المؤسسات الخاضعة للرقابة في المملكة، بما في ذلك الخدمات المالية والرعاية الصحية والجهات الحكومية. إن القدرة على تنفيذ تعليمات برمجية عن بُعد تعني أن المهاجمين قد يتمكنون من الوصول إلى بيانات حساسة أو تعديل معلومات عمل حرجية أو إنشاء وصول دائم داخل البيئة. المؤسسات التي تستخدم SharePoint في التكوينات السحابية أو التثبيتات المحلية معرضة للخطر ويجب عليها تقييم نماذج النشر الخاصة بها.

إرشادات المعالجة

أصدرت Microsoft تحديثات أمنية لمعالجة هذه الثغرة. يجب على المؤسسات تطبيق التحديثات المقدمة من المورد فوراً وفقاً لإجراءات إدارة التغيير الخاصة بها. بالنسبة لبيئات SharePoint السحابية، ينبغي للمؤسسات التحقق من أن مزود الخدمة قد طبق التحديثات اللازمة. إذا لم تكن الإجراءات التصحيحية متاحة لتكوينات معينة، يجب على المؤسسات تقييم إيقاف استخدام النسخ المتأثرة حتى تصبح التحديثات متاحة. يجب جرد جميع الأصول المتأثرة مع إيلاء اهتمام خاص لتلك المعرضة للإنترنت، وترتيب أولويات التحديثات بناءً على تقييم المخاطر والأهمية للأعمال.

ما يجب فعله الآن

1. جرد جميع نسخ Microsoft SharePoint في المؤسسة بما في ذلك البيئات السحابية والمحلية
2. تطبيق التحديثات الأمنية من Microsoft للثغرة CVE-2026-65660 فوراً وفقاً لإجراءات إدارة التغيير
3. بالنسبة لبيئات SharePoint السحابية، التحقق من مزودي الخدمة بأن التحديثات قد طبقت
4. تقييم مدى تعرض جميع أصول SharePoint للإنترنت وترتيب أولويات التحديثات بناءً على المخاطر والأهمية للأعمال
5. مراجعة سجلات الوصول لبيئات SharePoint للكشف عن أي نشاط مشبوه من المستخدمين المصرح لهم
6. في حال عدم توفر التحديثات لتكوينات معينة، تقييم العزل المؤقت أو إيقاف النسخ المتأثرة حتى تتوفر الإجراءات التصحيحية