

ثغرة اجتياز المسار في بوابة البريد الإلكتروني الآمنة من Cisco تتطلب تصحيحاً فورياً



تحتوي بوابة البريد الإلكتروني الآمنة من Cisco على ثغرة اجتياز مسار تتيح للمهاجمين عن بُعد دون مصادقة كتابة ملفات عشوائية على نظام التشغيل، مما يستوجب تطبيق التصحيحات الفورية.

- الثغرة CVE-2026-76519 تؤثر على بوابة البريد الإلكتروني الآمنة من Cisco بثغرة اجتياز مسار نسبي
- يمكن للمهاجمين عن بُعد دون مصادقة كتابة ملفات عشوائية على نظام التشغيل الأساسي
- يجب تطبيق تصحيحات المورد فوراً وفقاً لإرشادات التحديثات الأمنية القائمة على المخاطر
- على المؤسسات تقييم تعرض الأصول المتأثرة للإنترنت ووقف الاستخدام في حال عدم توفر التدابير الوقائية
- ينبغي اتباع إجراءات الفرز الجنائي للأنظمة المحتمل اختراقها

نظرة عامة على الثغرة

أعلنت Cisco عن الثغرة **CVE-2026-76519**، وهي ثغرة اجتياز مسار نسبي في بوابة البريد الإلكتروني الآمنة من Cisco تشكل خطراً كبيراً على المؤسسات التي تعتمد على حل أمن البريد الإلكتروني هذا. يتيح هذا العيب لمهاجم عن بُعد دون مصادقة كتابة ملفات عشوائية مباشرة على نظام التشغيل الأساسي دون الحاجة إلى بيانات اعتماد صالحة أو وصول مسبق إلى النظام.

هذا النوع من الثغرات مثير للقلق بشكل خاص للمؤسسات الخاضعة للتنظيم لأنه يتجاوز ضوابط المصادقة بالكامل ويمكن أن يمكّن المهاجمين من نشر تعليمات برمجية ضارة أو تعديل تكوينات النظام أو إنشاء آليات وصول دائمة على البوابات المتأثرة.

المخاطر على المؤسسات السعودية

تعمل بوابات البريد الإلكتروني كدفاعات محيطية حاسمة للمؤسسات المالية ومقدمي الرعاية الصحية والجهات الحكومية في جميع أنحاء المملكة. قد يؤدي الاستغلال الناجح إلى اختراق الاتصالات السرية أو تمكين الحركة الجانبية داخل الشبكات أو تسهيل أنشطة تسريب البيانات التي تنتهك المتطلبات التنظيمية بموجب أطر الهيئة الوطنية للأمن السيبراني ونظام حماية البيانات الشخصية.

يجب على المؤسسات التي تستخدم بوابة البريد الإلكتروني الآمنة من Cisco التعامل مع هذا الأمر كنشاط معالجة ذي أولوية. خاصة حيث تكون هذه الأنظمة معرضة للشبكات المواجهة للإنترنت أو تعالج اتصالات حساسة خاضعة للرقابة التنظيمية.

إرشادات المعالجة

يلزم اتخاذ إجراء فوري. يجب على المؤسسات تطبيق التصحيحات المقدمة من المورد وفقاً لتحديد الأولويات القائم على المخاطر، مع إعطاء الأولوية القصوى للأنظمة المعرضة للإنترنت. في حال عدم توفر التصحيحات بعد أو عدم إمكانية نشرها فوراً، يجب على المؤسسات تقييم التدابير البديلة بما في ذلك تجزئة الشبكة أو قيود الوصول أو التوقف المؤقت عن الخدمة حتى اكتمال المعالجة. يجب إخضاع الأنظمة التي ربما تعرضت قبل التصحيح للفرز الجنائي لتحديد مؤشرات الاختراق المحتملة.

ما يجب فعله الآن

1. تحديد جميع عمليات نشر بوابة البريد الإلكتروني الآمنة من Cisco في بيئتك وتقييم حالة تعرضها للإنترنت
2. تطبيق التصحيحات الأمنية المقدمة من المورد فوراً مع إعطاء الأولوية للأنظمة المواجهة للإنترنت وتلك التي تعالج بيانات خاضعة للتنظيم
3. تنفيذ تجزئة الشبكة أو قيود التحكم في الوصول كتدابير مؤقتة إذا لم يكن التصحيح الفوري ممكناً
4. إجراء فرز جنائي على الأنظمة التي تعرضت قبل التصحيح لتحديد مؤشرات الاختراق المحتملة
5. مراجعة وتحديث إجراءات الاستجابة للحوادث لمعالجة سيناريوهات استغلال اجتياز المسار
6. وقف استخدام الأنظمة المتأثرة إذا لم تكن تدابير المورد متاحة ولا يمكن نشر حلول بديلة آمنة لبوابة البريد الإلكتروني