

ثغرة اجتياز المسار في Fortinet FortiMail تتيح كتابة ملفات عشوائية



ثغرة اجتياز المسار في Fortinet FortiMail تسمح للمهاجمين غير المصادق عليهم بكتابة ملفات عشوائية على النظام عبر طلبات HTTP أو HTTPS مصممة خصيصاً.

- الثغرة CVE-2026-104286 تؤثر على Fortinet FortiMail بعيب اجتياز المسار ومعادلة البايث الفارغ
- يمكن للمهاجمين غير المصادق عليهم كتابة ملفات عشوائية على النظام الأساسي
- يحدث الاستغلال عبر طلبات HTTP أو HTTPS مصممة خصيصاً
- يجب على المؤسسات تطبيق تدابير التخفيف من المورد أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- الأصول المعرضة للإنترنت تتطلب تقييماً فورياً ومعالجة ذات أولوية

نظرة عامة على الثغرة

كشفت Fortinet عن ثغرة اجتياز المسار في FortiMail، المصنفة تحت الرقم CVE-2026-104286، والتي تسمح للمهاجمين غير المصادق عليهم بكتابة ملفات عشوائية على النظام الأساسي. يجمع العيب بين اجتياز المسار والمعالجة غير الصحيحة للبايت الفارغ أو الحرف الفارغ، مما يتيح الاستغلال عبر طلبات HTTP أو HTTPS مصممة خصيصاً دون الحاجة إلى بيانات اعتماد المصادقة.

تمثل هذه الثغرة خطراً كبيراً على المؤسسات التي تعتمد على FortiMail لأمن البريد الإلكتروني، خاصة تلك التي لديها عمليات نشر موجهة للإنترنت. قد يسمح الاستغلال الناجح للمهاجمين بوضع ملفات ضارة في دلائل النظام الحرجة، مما قد يؤدي إلى تنفيذ التعليمات البرمجية أو تصعيد الامتيازات أو الاختراق المستمر.

إرشادات المعالجة

يتعين على المؤسسات تطبيق تدابير التخفيف وفقاً لتعليمات المورّد فوراً. وفي حال عدم توفر تحديثات أو تدابير تخفيف من المورّد، يجب على المؤسسات تقييم إيقاف استخدام المنتج المتأثر، خاصة للحالات المعرضة للإنترنت. يؤكد التنبيه على أهمية تقييم تعرض كل أصل للإنترنت وتحديد أولويات المعالجة بناءً على المخاطر.

الاعتبارات التنظيمية

بالنسبة للمؤسسات الخاضعة للتنظيم في المملكة العربية السعودية، تتطلب هذه الثغرة إجراءً سريعاً بموجب أطر إدارة الثغرات المعتمدة. يجب على المؤسسات توثيق أنشطة المعالجة وتقييم التعرض المحتمل للبيانات الحساسة ومراجعة إجراءات الاستجابة للحوادث. غالباً ما تعالج أجهزة أمن البريد الإلكتروني اتصالات سرية وبيانات شخصية، مما يجعل التحديث في الوقت المناسب أمراً ضرورياً للامتثال التنظيمي والتزامات حماية البيانات.

ما يجب فعله الآن

1. تحديد جميع عمليات نشر Fortinet FortiMail في بيئتك مع إعطاء الأولوية للحالات الموجهة للإنترنت
2. تطبيق التحديثات أو تدابير التخفيف المقدمة من المورّد فوراً وفقاً لنشرات Fortinet الأمنية
3. تقييم إيقاف استخدام أنظمة FortiMail المتأثرة إذا لم تكن تدابير التخفيف من المورّد متاحة أو لا يمكن تطبيقها بسرعة
4. مراجعة السجلات للبحث عن طلبات HTTP/HTTPS مشبوهة أو نشاط إنشاء ملفات غير متوقع على أنظمة FortiMail
5. توثيق أنشطة المعالجة والجداول الزمنية للامتثال لمتطلبات إدارة الثغرات في الضوابط الأساسية للأمن السيرياني
6. تقييم ما إذا كانت أي بيانات حساسة أو معلومات خاضعة للتنظيم قد تعرضت وبدء إجراءات الاستجابة للحوادث في حال الاشتباه بحدوث اختراق