

ثغرة حرجة في بوابة البريد الإلكتروني الآمنة من سيسكو تتعرض لهجمات نشطة



أكدت سيسكو استغلالاً نشطاً لثغرة حرجة في بوابة البريد الإلكتروني الآمنة تتيح لمهاجمين غير مصادق عليهم كتابة ملفات على نظام التشغيل عبر مرفقات بريد إلكتروني مصممة خصيصاً، مما قد يؤدي إلى تنفيذ أوامر بصلاحيات الجذر.

- ثغرة حرجة في بوابة البريد الإلكتروني الآمنة من سيسكو تتعرض لاستغلال نشط
- يمكن للمهاجمين إرسال مرفقات بريد إلكتروني مصممة خصيصاً لكتابة ملفات على نظام تشغيل الجهاز دون مصادقة
- الاستغلال الناجح يتيح تنفيذ أوامر بصلاحيات الجذر على البوابة
- الجهاز مصمم لتصفية البريد الإلكتروني المؤسسي من الرسائل المزعجة والبرمجيات الخبيثة

تفاصيل الثغرة

أصدرت سيسكو تنبيهاً أمنياً يؤكد الاستغلال النشط لثغرة حرجة تؤثر على أجهزة بوابة البريد الإلكتروني الآمنة الخاصة بها. تتيح الثغرة لمهاجم غير مصادق عليه كتابة ملفات عشوائية على نظام التشغيل عبر إرسال بريد إلكتروني يحتوي على مرفق مصمم خصيصاً عبر البوابة. لا يتطلب استغلال هذه الثغرة أي بيانات اعتماد تسجيل دخول.

بمجرد معالجة المرفق الخبيث من قبل البوابة، يمكن للمهاجمين تنفيذ أوامر بصلاحيات الجذر على الجهاز المخترق. وهذا يمثل اختراقاً كاملاً لجهاز الأمان المصمم لحماية البنية التحتية للبريد الإلكتروني المؤسسي من الرسائل المزججة والبرمجيات الخبيثة.

التداعيات على أمن البريد الإلكتروني

تعتبر الثغرة مثيرة للقلق بشكل خاص لأنها تستهدف ضابطاً أمنياً تعتمد عليه المؤسسات كخط دفاع أول ضد التهديدات المنقولة عبر البريد الإلكتروني. قد تتيح بوابة البريد الإلكتروني المخترقة للمهاجمين اعتراض الاتصالات الحساسة أو تعديل قواعد التصفية للسماح برسائل البريد الإلكتروني الخبيثة أو استخدام الجهاز كنقطة ارتكاز لمزيد من الاختراق للشبكة.

نظراً للاستغلال النشط المؤكد، تواجه المؤسسات التي تشغل أجهزة بوابة البريد الإلكتروني الآمنة من سيسكو خطراً فورياً ويجب أن تتعامل مع هذا كحدث ذي أولوية يتطلب استجابة عاجلة.

استجابة فورية مطلوبة

نشرت سيسكو تنبيهاً يوضح تفاصيل الثغرة. يجب على المؤسسات الرجوع إلى الإرشادات الرسمية من سيسكو للحصول على التحديثات الأمنية أو التدابير التخفيفية المتاحة وتطبيقها دون تأخير على جميع نسخ المنتج المتأثر المنشورة.

ما يجب فعله الآن

1. تحديد جميع أجهزة بوابة البريد الإلكتروني الآمنة من سيسكو المنشورة في بيئتك فوراً والتحقق من إصدارات برامجها
2. الرجوع إلى التنبيه الأمني الرسمي من سيسكو لمعرفة توفر التحديثات الأمنية وتطبيقها على جميع النسخ المتأثرة كتغيير طارئ
3. في حال عدم توفر التحديثات الأمنية فوراً، تطبيق أي تدابير تخفيفية مؤقتة توصي بها سيسكو والنظر في عزل الأجهزة المتأثرة
4. مراجعة سجلات بوابة البريد الإلكتروني بحثاً عن مؤشرات الاختراق، خاصة نشاط كتابة الملفات غير المعتاد أو الأوامر الإدارية غير المتوقعة
5. إخطار فريق الاستجابة للحوادث لديكم والتصعيد للقيادة التنفيذية نظراً للطبيعة الحرجة والاستغلال النشط
6. التنسيق مع فريق حساب سيسكو الخاص بكم أو شريك الدعم المعتمد للحصول على المساعدة الفنية والإرشادات الخاصة ببيئتك