ثغرة حرجة في Cisco Secure Email Gateway قيد الاستغلال الفعلي



أفاد CERT-EU بأن الثغرة CVE-2026-76519 (CVSS 9.8) في Cisco Secure Email Gateway تتيح لمهاجم غير موثق تنفيذ أوامر بصلاحيات الجذر، وسيسكو على علم باستغلالها فعليًا. يلزم التحديث وفحص الأجهزة.

- الثغرة CVE-2026-76519 بدرجة CVSS تبلغ 9.8 وتؤثر في ميزة Advanced Malware Protection.
- يمكن لمهاجم عن بُعد دون مصادقة كتابة ملفات وتنفيذ أوامر بصلاحيات الجذر عبر مرفق بريد مُعدّ خصيصًا.
- فريق Cisco PSIRT على علم باستغلال الثغرة فعليًا.
- يشترط التأثر تفعيل File Reputation في سياسة بريد، وإصدار Content Scanner Tools أقدم من 25.3.0.5525.
- قد تُكشف مفاتيح SSH المستخدمة بين أعضاء العنقود على جهاز مخترَق.

نشرت Cisco في 14 أكتوبر 2026 نشرة أمنية بشأن ثغرة حرجة في ميزة Advanced Malware Protection (AMP) ضمن Cisco Secure Email Gateway. وأعاد CERT-EU نشر التنبيه في اليوم التالي، مشيرًا إلى أن Cisco PSIRT على علم باستغلالها فعليًا.

ما الذي تتيحه الثغرة

الثغرة (CVSS 9.8) CVE-2026-76519) هي خلل من نوع relative path traversal ناتج عن معالجة غير سليمة لمرفقات البريد عند تفعيل خدمة سمعة الملفات. يرسل المهاجم رسالة تحمل مرفقًا مُعدًّا خصيصًا عبر جهاز معرّض، فيستطيع كتابة ملفات تعسفية وتنفيذ أوامر بصلاحيات الجذر دون مصادقة.

وتشير Cisco إلى أن الأجهزة قد تعمل ضمن عناقيد. وعلى جهاز مخترق قد يمكن الوصول إلى مفاتيح SSH الخاصة المستخدمة بين أعضاء العنقود، ما قد يتيح اختراق بقية الأعضاء. وقد يزيل المهاجمون كذلك أدلة الاستغلال أو يخفونها.

الأجهزة المتأثرة

يشمل التأثر الأجهزة المادية والافتراضية التي تعمل بإصدارات AsyncOS من 15.5 قبل 15.5.5-014، أو 16.0، أو 16.5 قبل 16.5.0-780، بشرط تفعيل File Reputation وربطها بسياسة بريد، وأن يكون إصدار Content Scanner Tools أقدم من 25.3.0.5525. ولا تتأثر Secure Email and Web Manager ولا Secure Web Appliance. أما عملاء Secure Email Cloud Gateway فلا إجراء مطلوبًا منهم لأن الحزمة المصححة منشورة لديهم.

الاستجابة المقترحة

يحث CERT-EU على تحديث Content Scanner Tools أو ترقية AsyncOS بأسرع وقت، بدءًا بالأجهزة المكشوفة للإنترنت. وتوصي Cisco بمراجعة سجلات النظام في كل جهاز بحثًا عن رسائل الاشتباه بالاختراق. ولأن صلاحيات الجذر تتيح إخفاء الآثار، توصي كذلك بمطابقة سجلات الشبكة والجدار الناري خارج الجهاز بحثًا عن رفع غير متوقع إلى عناوين IP خارجية أو تنزيل من عناوين خبيثة. ولم تنشر Cisco مؤشرات اختراق محددة.

ما يجب فعله الآن

1. حصر جميع أجهزة Cisco Secure Email Gateway بما فيها أعضاء العناقيد، والتحقق من إصداري AsyncOS وContent Scanner Tools.
2. التأكد من تفعيل File Reputation وربطها بأي سياسة بريد.
3. تحديث Content Scanner Tools إلى 25.3.0.5525 أو أحدث، أو ترقية AsyncOS إلى إصدار مصحح، بدءًا بالأجهزة المكشوفة للإنترنت.
4. مراجعة سجلات النظام في كل جهاز بحثًا عن رسائل الاختراق التي وصفتها Cisco، وتفعيل خطة الاستجابة للحوادث عند رصد أي منها.
5. مطابقة سجلات الشبكة والجدار الناري بحثًا عن رفع غير متوقع إلى عناوين IP خارجية أو تنزيل من عناوين خبيثة.
6. عند اكتشاف اختراق أو الاشتباه به، فحص بقية أعضاء العنقود والتواصل مع Cisco TAC.