استغلال ثغرة Cisco Expressway رقم CVE-2026-76466 بُعيد نشر شيفرة إثبات المفهوم



استغل مهاجمون الثغرة الحرجة (CVSS 9.8) CVE-2026-76466 في Cisco Expressway ضد جهة روسية بعد وقت قصير من نشر شيفرة إثبات المفهوم. تتيح الثغرة استغلالًا عن بُعد دون مصادقة.

- الثغرة مسجلة بالرقم CVE-2026-76466 وتبلغ درجتها 9.8 وفق CVSS.
- يمكن لمهاجم عن بُعد دون مصادقة، لديه وصول شبكي إلى Cisco Expressway، استغلالها.
- رُصد الاستغلال ضد جهة روسية بعد وقت قصير من نشر شيفرة إثبات المفهوم علناً.
- يفيد عنوان الخبر باختراق أربعة أجهزة ووصول المهاجمين إلى الشبكة الداخلية.

ما الذي ورد في التقرير

رُصد مهاجمون يستغلون ثغرة حرجة أُعلن عنها حديثاً في Cisco Expressway، وهي مسجلة بالرقم

CVE-2026-76466 وتبلغ درجتها 9.8 وفق مقياس CVSS. ووفق التقرير، يمكن لمهاجم عن بُعد دون مصادقة، ولديه وصول شبكي إلى جهاز Expressway المتأثر، استغلال هذه الثغرة.

وقد استهدف النشاط جهة روسية، وجاء بعد وقت قصير من نشر شيفرة إثبات مفهوم علناً. ويذكر عنوان التقرير أن أربعة أجهزة اختُرقت، وأن المهاجمين وصلوا بعد ذلك إلى الشبكة الداخلية.

لماذا يهم ذلك

لا يتضمن المقتطف المتاح تفاصيل تقنية إضافية، مثل الإصدارات المتأثرة أو توفر التحديثات، لذا ينبغي الرجوع إلى نشرة Cisco الرسمية لمعرفتها. أما ما يبرزه التقرير فهو سرعة تحول الثغرة المعلنة إلى استغلال فعلي عند توفر شيفرة إثبات مفهوم علنية، وإمكانية أن يكون جهاز تعاون على حافة الشبكة بوابة إلى الأنظمة الداخلية.

ورغم أن الضحية المرصودة خارج المملكة، فإن أي جهة في السعودية تشغّل Cisco Expressway معنية بالأمر، خاصة إذا كانت الخدمة متاحة من الإنترنت.

الخطوات التالية

تأكدوا من وجود Expressway في بيئتكم، وحددوا مدى تعرضه، واتبعوا إرشادات Cisco للمعالجة. وراجعوا الأجهزة بحثاً عن مؤشرات اختراق، وافحصوا أي نشاط غير معتاد صادر عنها نحو الشبكات الداخلية.

ما يجب فعله الآن

1. حصر جميع أجهزة Cisco Expressway وتحديد ما يمكن الوصول إليه من الإنترنت.
2. مراجعة نشرة Cisco الخاصة بالثغرة CVE-2026-76466 وتطبيق التحديثات أو إجراءات التخفيف الموصى بها بأولوية عالية.
3. فحص سجلات Expressway وحالة الأجهزة بحثاً عن مؤشرات اختراق، والتعامل مع أي نتيجة مشبوهة بوصفها حادثاً.
4. مراقبة الاتصالات الصادرة من أجهزة Expressway نحو الشبكات الداخلية للكشف عن أي اتصال غير متوقع.
5. تقييد الوصول الشبكي إلى واجهات الإدارة والخدمة إلى الحد الأدنى اللازم لحين اكتمال المعالجة.