استغلال ثغرة CVE-2026-76466 Cisco Expressway بعد وقت قصير من نشر شيفرة الاستغلال



أفادت F6 بأن مهاجمين استغلوا الثغرة الحرجة CVE-2026-76466 في Cisco Expressway لاختراق جهة بعد وقت قصير من نشر شيفرة استغلال علنية. وتؤثر على الأجهزة العنقودية ولا يوجد حل بديل.

- تتيح الثغرة CVE-2026-76466 (درجة 9.8 CVSS) لمهاجم عن بُعد دون مصادقة تنفيذ أوامر بصلاحيات root على Expressway Core وEdge، وذلك عند تشغيل الأجهزة ضمن عنقود فقط.
- كشفت Cisco عن الثغرة في 21 أكتوبر، ويعالجها الإصدار Expressway X15.5.20، ولا توجد حلول بديلة.
- نُشرت شيفرة استغلال على GitHub، وتقول F6 إن الهجوم الذي حققت فيه وقع بعدها بوقت قصير.
- دخل المهاجمون عبر جهازين من الإصدار X15.5.3 معرّضين للإنترنت، ثم انتقلوا إلى عقدتين

داخليتين واستخدموا سكربتات Python مخصصة للحركة الجانبية.

- توصي F6 بفحص سجل Erlang، وبتقييد المنفذين 4372–4371 TCP على العقد الموثوقة إذا تأخر التحديث.

أفادت شركة الأمن السيبراني F6 بأن مهاجمين استغلوا ثغرة حرجة في Cisco Expressway لاختراق جهة بعد وقت قصير من نشر شيفرة إثبات المفهوم (PoC). ولم تذكر F6 اسم الضحية ولم تنسب النشاط إلى جهة تهديد معروفة.

ما هو معلوم

تتيح الثغرة **CVE-2026-76466** (درجة CVSS 9.8) لمهاجم عن بُعد يملك وصولًا إلى الشبكة تنفيذ أوامر بصلاحيات root دون مصادقة. وتؤثر في النسختين الافتراضية والمادية من Expressway Core وExpressway Edge، لكن عند تشغيلها ضمن عنقود فقط. وتقول Cisco إنها في خدمة قاعدة البيانات وترتبط بملفات تعريف الارتباط الدائمة، ما يتيح للمهاجم إصدار أوامر RPC معينة.

كشفت Cisco عن المشكلة في 21 أكتوبر. ولم يُحدَّث إشعارها منذ صدوره، وما زال يذكر أنها لا تعلم بأي استخدام خبيث، بينما ظهرت لاحقاً شيفرة PoC على GitHub. ووفق التقرير لم تعلّق Cisco بعد على نتائج F6.

كيف جرى الهجوم

تقول F6 إن المهاجمين اخترقوا جهازين من الإصدار Expressway X15.5.3 معرّضين للإنترنت، ثم انتقلوا إلى عقدتين أخريين في الشبكة الداخلية. وبعد الحصول على صلاحيات root أعدّوا سكربتات Python لمسح الشبكة وإيجاد موارد SMB والتفاعل مع SQL Server وWinRM والبحث في مستودعات GitLab عن بيانات اعتماد ومعلومات حساسة. وترجّح F6 أن السكربتات عُدّلت أثناء الهجوم وأن الشيفرة تحمل مؤشرات على استخدام مساعد ذكاء اصطناعي.

المعالجة والتخفيف

يعالج الإصدار Expressway X15.5.20 الثغرة. ولا تذكر Cisco حلولًا بديلة، ويتعين على عملاء X14 والإصدارات الأقدم الانتقال إلى إصدار مصحَّح. وتنصح F6 من لا يستطيع التحديث فوراً بحظر الاتصال بالمنفذين 4372–4371 TCP في جدار الحماية باستثناء عناوين العقد الموثوقة في العنقود، ومراجعة سجل Erlang بحثاً عن مؤشرات استغلال.

ما يجب فعله الآن

1. حصر جميع أجهزة Expressway Core وEdge وتحديد الموجود منها ضمن عنقود وتسجيل إصداراتها.
2. الترقية إلى X15.5.20 أو أحدث، والتخطيط للانتقال من X14 والإصدارات الأقدم لعدم وجود حل بديل.
3. عند تعذر التحديث فوراً، حظر المنفذين 4372–4371 TCP في جدار الحماية باستثناء عناوين العقد الموثوقة.
4. مراجعة سجل Erlang على الأجهزة والتحقق من عناوين IP ومسارات الملفات التي نشرتها F6.
5. البحث عن حركة جانبية باتجاه SMB وSQL Server وWinRM وGitLab، وتدوير بيانات الاعتماد عند الاشتباه بالاختراق.

6. تقليص تعرّض أجهزة Expressway للإنترنت إلى الحد اللازم للوصول التعاوني، بما يتسق مع ضوابط إدارة الثغرات والتحديثات في ضوابط الهيئة الوطنية للأمن السيبراني (ECC).