CISA تحذّر من استغلال فعلي لثغرتين في SAP NetWeaver وCisco Expressway



تفيد CISA بأن مهاجمين يستغلون ثغرة متوسطة الخطورة في SAP NetWeaver وأخرى حرجة في Cisco Expressway. التحديثات متاحة للثغرتين، وثغرة Expressway تمس الأجهزة المهيأة في عنقود.

- الثغرة CVE-2025-42884 في SAP NetWeaver (درجة CVSS 6.5) قد تتيح لمهاجم غير مصادق تسريب معلومات الخادم أو تعديلها، وقد أصدرت SAP إصلاحها في تحديثات نوفمبر 2025.
- الثغرة CVE-2026-76466 في Cisco Expressway (درجة CVSS 9.8) ضعف ناتج عن بيانات اعتماد مضمّنة، وقد تتيح تنفيذ أوامر على النظام بصلاحيات الجذر.
- تمس أجهزة Expressway-C وExpressway-E ذات الإصدارات المعرضة والمهيأة في عنقود، والإصلاح في الإصدار X15.5.20 الصادر في 21 أكتوبر.
- أضافت CISA ثغرة Expressway إلى كتالوج KEV في 20 نوفمبر ومنحت الجهات الاتحادية

الأمريكية ثلاثة أيام للتصحيح.

- أفادت شركة F6 ببدء الاستغلال بعد وقت قصير من نشر شيفرة إثبات المفهوم علنًا.

حذّرت الوكالة الأمريكية للأمن السيبراني CISA من أن مهاجمين يستغلون ثغرات في Ciscoو SAP NetWeaver Expressway. وتتوفر إصلاحات للثغرتين، لذا تتمثل الأولوية لدى معظم الجهات في التأكد من تطبيقها.

SAP NetWeaver

تبلغ درجة **CVE-2025-42884** وفق CVSS 6.5. وقد تتيح لمهاجم غير مصادق تسريب معلومات الخادم أو تعديلها، عبر حقن خصائص بيئة JNDI أو تمرير عنوان URL يُستخدم في عمليات البحث عبر JNDI، بما يقود إلى مزوّد JNDI غير مقصود. وقد عالجتها SAP في تحديثاتها الأمنية لشهر نوفمبر 2025. ولا يشير المصدر إلى تقارير سابقة عن استغلالها قبل تنبيه CISA.

Cisco Expressway

تصنَّف **CVE-2026-76466** حرجة بدرجة 9.8، وتنشأ من بيانات اعتماد مضمّنة. فاستخدام ملفات تعريف الارتباط الدائمة مع ضعف التحقق من شهادات العميل في ظروف معينة قد يتيح لمن يملك هذه الملفات الاتصال بخدمة قاعدة البيانات واستدعاء أوامر RPC محددة، وصولاً إلى تنفيذ أوامر على النظام بصلاحيات الجذر.

وتتأثر أجهزة Expressway Core (Expressway-C) وExpressway Edge (Expressway-E) عند تشغيل إصدارات معرضة وإعدادها في عنقود. وقد صدر الإصلاح في 21 أكتوبر ضمن الإصدار X15.5.20 من Expressway Series.

وأضافت CISA الثغرة إلى كتالوج الثغرات المستغلة المعروفة (KEV) في 20 نوفمبر، وحدّدت للجهات الاتحادية مهلة ثلاثة أيام. وكانت شركة F6 الروسية قد أفادت ببدء الاستغلال بعد وقت قصير من نشر شيفرة إثبات المفهوم.

الخلاصة

غالبًا ما يقع جهاز Expressway على حدود الشبكة، ما يجعل ثغرة حرجة مع شيفرة استغلال علنية جديرة بمراجعة عاجلة. أما ثغرة SAP فأقل تصنيفًا، لكن الاستغلال الفعلي يبرر التحقق من حالة التصحيح فيها أيضًا.

ما يجب فعله الآن

1. حصر جميع أجهزة Cisco Expressway-C وExpressway-E والتحقق من تشغيلها إصدارًا أقدم من X15.5.20، خاصة المهيأة في عنقود.
2. تطبيق إصلاح Expressway كتغيير طارئ ومراجعة السجلات بحثًا عن نشاط غير متوقع في خدمة قاعدة البيانات أو أوامر RPC.
3. التأكد من تطبيق تحديثات SAP الأمنية لنوفمبر 2025 على أنظمة NetWeaver، ومنها معالجة CVE-2025-42884.
4. اعتماد كتالوج KEV لدى CISA مدخلاً في ترتيب أولويات معالجة الثغرات، بحيث تُصحَّح الثغرات المستغلة قبل غيرها مهما كانت درجة CVSS.

5. توثيق حالة التعرض والمعالجة في سجل المخاطر، والإبلاغ عن أي اشتباه باختراق عبر إجراءات الاستجابة للحوادث.