CISA تحذّر من ثغرة CVE-2025-42884 في SAP NetWeaver Enterprise Portal



أدرجت CISA الثغرة CVE-2025-42884 في SAP NetWeaver Enterprise Portal، وتتيح لمهاجم غير موثّق كشف معلومات الخادم أو تعديلها عبر التلاعب بعمليات JNDI. يُنصح بالتخفيف وفق تعليمات SAP.

- الثغرة CVE-2025-42884 تؤثر في SAP NetWeaver Enterprise Portal.
- سببها عدم تعقيم العناصر الخاصة بصورة سليمة في منطق استعلام البيانات.
- يمكن لمهاجم غير موثّق كشف معلومات الخادم أو تعديلها.
- يتم الهجوم عبر خصائص بيئة JNDI المحقونة أو عنوان URL يُستخدم في عمليات البحث عبر JNDI.
- الموعد النهائي لدى الجهات الفدرالية الأمريكية هو 23-11-2026، وتشير CISA إلى توجيه BOD 26-04 ومتطلبات الفرز الجنائي.

ما الذي أُعلن

أدرجت CISA الثغرة CVE-2025-42884 في SAP NetWeaver Enterprise Portal. وتوصَف بأنها عدم تعقيم سليم للعناصر الخاصة في منطق استعلام البيانات، ويمكن لمهاجم غير موثّق استغلالها لكشف معلومات على الخادم أو تعديلها.

تقوم الطريقة على حقن خصائص بيئة JNDI، أو تمرير عنوان URL يُستخدم أثناء عملية بحث عبر JNDI. ولأن الاستغلال لا يتطلب مصادقة، فإن أي نسخة يمكن الوصول إليها من المهاجم تستدعي الانتباه.

ما تطلبه CISA

تطلب CISA تطبيق إجراءات التخفيف وفق تعليمات الجهة المصنِّعة، بما يتوافق مع توجيهها BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر، ومع متطلبات الفرز الجنائي (Forensics Triage Requirements). وإذا لم تتوفر إجراءات تخفيف، فيُتّبع ما ينطبق من BOD 26-04 على الخدمات السحابية أو يُوقف استخدام المنتج. وتقع على الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت. أما الموعد النهائي للجهات الفدرالية فهو 2026-11-23.

لا يذكر المصدر أرقام الإصدارات المتأثرة ولا تفاصيل الاستغلال، لذا ينبغي الرجوع إلى إشعار SAP نفسه لمعرفتها.

قراءة عملية للمؤسسات في المملكة

ينطبق الموعد على الجهات الفدرالية الأمريكية، لكن منطق المخاطر يسري على أي جهة تشغّل Enterprise Portal. يبدأ العمل بتحديد أماكن نشر البوابة ومدى تعرضها للإنترنت، ثم تطبيق إجراءات SAP وحفظ الأدلة لأغراض التدقيق.

ما يجب فعله الآن

1. حصر جميع نسخ SAP NetWeaver Enterprise Portal وتحديد ما هو متاح منها من الإنترنت.
2. تطبيق إجراءات التخفيف التي نشرتها SAP للثغرة CVE-2025-42884 وتوثيق التغيير.
3. إعطاء الأولوية للنسخ المواجهة للإنترنت، وتقييد الوصول إليها مؤقتًا متى أمكن حتى اكتمال المعالجة.
4. مراجعة سجلات البوابة والخادم بحثًا عن طلبات غير معتادة متعلقة بـ JNDI، وحفظ الأدلة عند رصد أي أثر.
5. رفع الموضوع ضمن إدارة الثغرات وإبلاغ مسؤول الأمن السيبراني بالحالة وفق عمليات NCA ECC وSAMA CSF.