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



أدرجت CISA الثغرة CVE-2025-42884 في SAP NetWeaver Enterprise Portal، وهي تتيح لمهاجم غير موثّق الاطلاع على معلومات الخادم أو تعديلها عبر عمليات JNDI. يلزم تطبيق معالجات الشركة المصنّعة ومراجعة التعرض للإنترنت.

- تؤثر الثغرة في SAP NetWeaver Enterprise Portal، وتتعلق بعدم تنقية العناصر الخاصة بصورة سليمة في منطق استعلام البيانات.
- يمكن لمهاجم غير موثّق الاطلاع على معلومات الخادم أو تعديلها.
- يتم الاستغلال عبر خصائص بيئة JNDI المحقونة أو عنوان URL يُستخدم في عمليات البحث عبر JNDI.
- تشترط CISA تطبيق معالجات الشركة المصنّعة والالتزام بتوجيه BOD 26-04 ومتطلبات الفرز الجنائي، والموعد الاتحادي هو 23-11-2026.

- عند تعذّر المعالجات تدعو CISA إلى التوقف عن استخدام المنتج.

أدرجت CISA الثغرة CVE-2025-42884 ضمن قائمتها، وتصفها بأنها عدم تنقية سليمة للعناصر الخاصة في منطق استعلام البيانات داخل SAP NetWeaver Enterprise Portal.

ما الذي تتيحه الثغرة

يستطيع مهاجم غير موثّق الاطلاع على معلومات مخزنة على الخادم أو تعديلها. ويتم ذلك عبر حقن خصائص بيئة JNDI، أو عنوان URL يُستخدم أثناء عملية بحث JNDI. ولا يحتاج المهاجم إلى بيانات اعتماد، ما يجعل أي نسخة من البوابة يمكن الوصول إليها مصدر قلق.

ما تطلبه CISA

توجّه CISA الجهات إلى تطبيق المعالجات وفق تعليمات الشركة المصنّعة، وبما يتوافق مع توجيهها BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر، ومع متطلبات الفرز الجنائي لديها. وفي الخدمات السحابية يُتّبع التوجيه المعني من BOD 26-04. وإذا لم تتوفر معالجات فينبغي التوقف عن استخدام المنتج. وتقع على أصحاب الشأن مسؤولية تقييم تعرّض كل أصل للإنترنت والالتزام بمهل التحديث. والموعد الاتحادي هو 2026-11-23.

القراءة العملية للجهات في المملكة

يستهدف التوجيه الجهات الاتحادية الأمريكية، لكن الخطر التقني قائم لأي جهة تشغّل SAP NetWeaver Enterprise Portal. ولا يذكر المصدر الإصدارات المتأثرة ولا أرقام التحديثات، لذا يُرجع إلى إشعار SAP نفسه لهذه التفاصيل. والبداية تحديد أماكن تشغيل البوابة وهل يمكن الوصول إليها من الإنترنت، ثم تطبيق معالجات الشركة والتحقق من أي مؤشرات على إساءة الاستخدام.

ما يجب فعله الآن

1. حصر جميع نسخ SAP NetWeaver Enterprise Portal وتحديد ما يمكن الوصول إليه من الإنترنت.
2. تطبيق المعالجات الواردة في تعليمات SAP مع إعطاء الأولوية للنسخ المكشوفة للإنترنت.
3. عند تعذّر المعالجات، التخطيط لتقييد الوصول أو إيقاف استخدام المكوّن كما توصي CISA.
4. مراجعة سجلات البوابة والخادم بحثاً عن عمليات بحث JNDI غير معتادة أو طلبات URL صادرة غير متوقعة.
5. توثيق تقييم التعرض والمعالجة ضمن إدارة الثغرات ورفعها إلى مسؤول أمن المعلومات.