

SAP تعالج ثغرة بحد أقصى للخطورة في OAuth2 تتيح سرقة بيانات الاعتماد في Cloud SDK for Python



أصدرت SAP تحديثاً أمنياً لمعالجة الثغرة CVE-2026-89111 ذات الخطورة القصوى في OAuth2 SSRF ضمن Cloud SDK for Python والتي تتيح للمهاجمين عن بُعد سرقة بيانات الاعتماد من تطبيقات BTP متعددة المستأجرين.

- الثغرة CVE-2026-89111 هي ثغرة OAuth2 SSRF بحد أقصى للخطورة في SAP Cloud SDK for Python تؤثر على تطبيقات BTP متعددة المستأجرين
- يمكن للمهاجمين عن بُعد استغلال الثغرة دون امتيازات عبر التحكم في معامل tenant_subdomain لإعادة توجيه طلبات رموز OAuth2 وسرقة بيانات اعتماد العميل
- أصدرت SAP تحديثات أمنية لشهر أكتوبر 2026 تعالج 20 ثغرة عبر منتجات متعددة، بما في ذلك ثغرتان إضافيتان بخطورة درجة
- يتوفر تخفيف مؤقت عبر التحقق من صحة قيم tenant_subdomain باستخدام قائمة مسموح بها

للمؤسسات غير القادرة على التحديث فوراً

- أدرجت CISA الأمريكية 14 ثغرة في SAP كـثغرات مستغلة فعلياً منذ نوفمبر 2021، ثلاث منها استُخدمت في حملات برمجيات الفدية

تفاصيل الثغرة الأمنية

أصدرت SAP تحديثاتها الأمنية لشهر أكتوبر 2026 لمعالجة 20 ثغرة عبر محفظة منتجاتها، تصدرها الثغرة CVE-2026-89111 ذات الخطورة القصوى في Cloud SDK for Python. يعمل هذا SDK كمجموعة أدوات برمجية رسمية لتطوير وكلاء الذكاء الاصطناعي وتطبيقات Python على خدمات منصة SAP Business Technology Platform.

تؤثر ثغرة **OAuth2 SSRF** على تطبيقات BTP متعددة المستأجرين ويمكن استغلالها من قبل مهاجمين عن بُعد دون الحاجة إلى أي امتيازات. من خلال التحكم في معامل `tenant_subdomain`، يستطيع المهاجمون إعادة توجيه طلبات رموز OAuth2 إلى خوادم تحت سيطرتهم، مما يتسبب في استخراج بيانات اعتماد العميل. أكدت SAP أن المؤسسات غير القادرة على نشر التحديثات فوراً يمكنها التخفيف المؤقت من المخاطر عبر التحقق من صحة قيم `tenant_subdomain` مقابل قائمة معروفة من نطاقات المستأجرين المسجلة قبل تمريرها إلى استدعاءات SDK.

ثغرات حرجية إضافية تمت معالجتها

يعالج تحديث أكتوبر أيضاً الثغرة CVE-2026-89110، وهي ثغرة حرجية في التحكم بالوصول المعطل في SAP NetWeaver Visual Composer تسمح للمهاجمين عن بُعد بامتيازات محدودة باختراق الأنظمة الضعيفة بالكامل. تؤثر ثغرة حرجية ثالثة CVE-2026-89108 على SAP Manufacturing Integration and Intelligence، مما يتيح للجهات المهددة بامتيازات المسؤول توفير حسابات بامتيازات مرتفعة على تطبيق Java الأساسي والحصول على تحكم إداري بالنظام.

السياق الأوسع

عاجت SAP عدة ثغرات بحد أقصى للخطورة في الأشهر الأخيرة، بما في ذلك CVE-2026-58231 في Commerce Cloud في أغسطس، والتي تم الإبلاغ عن استغلالها فعلياً بعد فترة وجيزة من الإفصاح عنها. أدرجت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية 14 ثغرة أمنية في SAP كـثغرات مستغلة فعلياً منذ نوفمبر 2021، مع تأكيد استخدام ثلاث منها في هجمات برمجيات الفدية. تخدم 99 SAP من أكبر 100 شركة في العالم وأعلنت عن إيرادات تتجاوز 36 مليار يورو في السنة المالية 2025.

ما يجب فعله الآن

1. تحديد جميع عمليات نشر SAP Cloud SDK for Python وتطبيقات BTP متعددة المستأجرين ضمن بيئتك فوراً
2. تطبيق تحديثات SAP الأمنية لشهر أكتوبر 2026 للثغرات CVE-2026-89111 و CVE-2026-89110 و CVE-2026-89108 كأولوية
3. في حال تعذر التحديث الفوري، تنفيذ التحقق من صحة قيم `tenant_subdomain` باستخدام قائمة مسموح بها قبل تمريرها إلى استدعاءات SDK

4. مراجعة ضوابط الوصول وتعيينات الامتيازات للأنظمة SAP و SAP NetWeaver Visual Composer
Manufacturing Integration and Intelligence

5. مراقبة أنماط طلبات رموز OAuth2 واستخدام بيانات الاعتماد للكشف عن الشذوذات التي قد تشير إلى محاولات استغلال

6. التنسيق مع فريق دعم SAP للتحقق من نشر التحديثات وتأكيد فعالية التخفيف عبر جميع الأنظمة المتأثرة