

ثغرة تثبيت الجلسة في Zammad تتيح تنفيذ التعليمات البرمجية عن بُعد



تحتوي منصة Zammad من شركة Zammad GmbH على ثغرة تثبيت جلسة قد تؤدي إلى تنفيذ تعليمات برمجية عن بُعد بصلاحيات مستخدم النظام ويمكن ربطها مع ثغرة أخرى.

- منصة Zammad من Zammad GmbH تحتوي على ثغرة تثبيت جلسة مسجلة برقم CVE-2026-102489
- يمكن للثغرة أن تؤدي إلى تنفيذ تعليمات برمجية عن بُعد بصلاحيات مستخدم zammad
- يمكن ربط الثغرة مع CVE-2026-102490 لتأثير أكبر محتمل
- يجب تطبيق إجراءات المعالجة من المورّد فوراً أو إيقاف استخدام المنتج في حال عدم توفر التحديثات
- على المؤسسات تقييم مدى تعرض الأصول المتأثرة للإنترنت وإعطاء الأولوية للتحديثات الأمنية

نظرة عامة على الثغرة

تحتوي منصة Zammad من شركة Zammad GmbH، وهي نظام ويب لدعم العملاء وإدارة التذاكر، على ثغرة تثبيت جلسة مصنفة برقم CVE-2026-102489. تتيح هذه الثغرة الأمنية للمهاجمين إمكانية تنفيذ تعليمات برمجية عشوائية عن بُعد بصلاحيات حساب مستخدم zammad. تصبح الثغرة أكثر خطورة عند دمجها مع الثغرة CVE-2026-102490، مما يمكن المهاجمين من ربط الثغرات لاختراق أكثر خطورة.

تحدث هجمات تثبيت الجلسة عندما يتمكن المهاجم من فرض معرّف جلسة المستخدم إلى قيمة معروفة، مما يسمح للمهاجم باختطاف الجلسات المصادق عليها. في هذه الحالة، يمنح الاستغلال الناجح قدرات تنفيذ التعليمات البرمجية، مما يمثل خطراً كبيراً على سرية وسلامة وتوافر الأنظمة المتأثرة.

سياق المخاطر للمؤسسات السعودية

يجب على المؤسسات التي تستخدم Zammad لعمليات خدمة العملاء أو إدارة خدمات تقنية المعلومات أو نظام التذاكر الداخلي أن تتعامل مع هذه الثغرة على أنها تتطلب اهتماماً فورياً. إن إمكانية تنفيذ التعليمات البرمجية عن بُعد تعني أن المهاجمين قد يحصلون على وصول غير مصرح به إلى بيانات العملاء الحساسة أو تذاكر الدعم التي تحتوي على معلومات سرية، أو استخدام الأنظمة المخترقة كنقاط ارتكاز لاختراق أوسع للشبكة.

يجب على الجهات الخاضعة للتنظيم في المملكة تقييم ما إذا كانت نسخ Zammad معرضة للإنترنت وتقييم حساسية البيانات المعالجة عبر هذه الأنظمة. إن القدرة على ربط هذه الثغرة مع CVE-2026-102490 تزيد من إلحاح جهود المعالجة.

الاستجابة الموصى بها

يجب على المؤسسات استشارة إرشادات المورد Zammad GmbH فوراً للحصول على التحديثات الأمنية المتاحة وتطبيق التصحيحات دون تأخير. إذا لم تكن إجراءات المعالجة متاحة من المورد، يجب على المؤسسات النظر في إيقاف استخدام المنتج حتى صدور التصحيحات. يجب على مالكي الأصول إجراء فحص جنائي إذا كان هناك اشتباه في حدوث اختراق وتوثيق جميع أنشطة المعالجة لأغراض الامتثال.

ما يجب فعله الآن

1. تحديد جميع نسخ Zammad المنشورة في مؤسستك وتوثيق حالة تعرضها للإنترنت
2. استشارة نشرات الأمن السيرياني من المورد Zammad GmbH فوراً للحصول على التصحيحات المتاحة وإرشادات المعالجة
3. تطبيق التحديثات الأمنية المقدمة من المورد على جميع تثبيتات Zammad المتأثرة كنشاط معالجة ذي أولوية
4. في حال عدم توفر التصحيحات، تقييم إيقاف استخدام Zammad حتى صدور إجراءات المعالجة من المورد
5. إجراء فحص جنائي على أنظمة Zammad في حال الاشتباه بوصول غير مصرح به أو نشاط غير طبيعي
6. مراجعة سجلات الوصول وسجلات إدارة الجلسات للبحث عن مؤشرات تثبيت الجلسة أو محاولات الاستغلال