

ثغرة تصعيد الصلاحيات في منصة زماد لإدارة طلبات الدعم



ثغرة في إدارة الصلاحيات بمنصة زماد تتيح للمستخدمين المحليين تصعيد الصلاحيات إلى مستوى الجذر، مما قد يؤدي إلى اختراق كامل للنظام عند ربطها بثغرة أخرى.

- الثغرة CVE-2026-102490 تؤثر على منصة زماد لإدارة طلبات الدعم مع خلل في إدارة الصلاحيات
- حسابات المستخدمين المحليين يمكنها تصعيد الصلاحيات إلى مستوى الجذر
- يمكن ربط الثغرة مع CVE-2026-102489 لتأثير أكبر
- يجب على المؤسسات تطبيق تدابير المورّد أو إيقاف استخدام المنتج
- النسخ المعرضة للإنترنت تتطلب تقييماً وتحديثاً فوراً

نظرة عامة على الثغرة

تحتوي منصة زمامد من شركة Zammad GmbH، وهي نظام منتشر على نطاق واسع لإدارة طلبات الدعم وخدمة العملاء، على ثغرة في إدارة الصلاحيات مسجلة برقم **CVE-2026-102490**. يسمح هذا الخلل لمستخدم محلي بصلاحيات مستوى زمامد بتعديل صلاحياته إلى مستوى الجذر، مما يمنحه سيطرة إدارية كاملة على النظام المتأثر. تصبح الثغرة مثيرة للقلق بشكل خاص عند دمجها مع CVE-2026-102489، حيث تمكّن المهاجمين من ربط عدة ثغرات لاختراق أوسع للنظام.

المخاطر على المؤسسات الخاضعة للتنظيم

بالنسبة للمؤسسات التي تشغل نسخ زمامد في بيئات خدمة العملاء أو الدعم التقني أو تقنية العمليات، تمثل هذه الثغرة خطراً أمنياً كبيراً. يمكن أن يتيح تعديل الصلاحيات إلى مستوى الجذر وصولاً غير مصرح به إلى بيانات العملاء الحساسة وتذاكر الدعم التي تحتوي على معلومات سرية والأنظمة الخلفية المتصلة المحتملة. يجب على المؤسسات الخاضعة للأطر التنظيمية بما في ذلك ضوابط حماية البيانات والأمن السيبراني معاملة هذا الأمر كبند معالجة ذي أولوية.

إرشادات المعالجة

يجب على المؤسسات الرجوع فوراً إلى وثائق المورد Zammad GmbH للحصول على التحديثات الأمنية المتاحة وتطبيق الرقع وفقاً لإجراءات إدارة التغيير الخاصة بها. حيثما تكون نسخ زمامد معرضة للإنترنت أو يمكن الوصول إليها من شبكات غير موثوقة، يجب إعطاء الأولوية للترقيع السريع أو العزل المؤقت. إذا لم تكن تدابير المورد متاحة أو لا يمكن تطبيقها ضمن أطر زمنية مقبولة، يجب على المؤسسات تقييم حلول بديلة لإدارة طلبات الدعم. يجب توثيق جميع أنشطة المعالجة لأغراض الامتثال والمراجعة، مع إيلاء اهتمام خاص للأنظمة التي تعالج بيانات خاضعة للتنظيم.

ما يجب فعله الآن

1. تحديد جميع نسخ منصة زمامد المنشورة في المؤسسة، بما في ذلك بيئات الإنتاج والاختبار والتطوير
2. الرجوع إلى نشرات المورد Zammad GmbH الأمنية للحصول على الرقع المعالجة لـ CVE-2026-102490 و CVE-2026-102489
3. إعطاء الأولوية لترقيع نسخ زمامد المعرضة للإنترنت أو التي يمكن الوصول إليها خارجياً خلال 72 ساعة
4. مراجعة سجلات الوصول لحسابات مستخدمي زمامد للكشف عن محاولات تعديل صلاحيات غير مصرح بها محتملة
5. تطبيق تجزئة الشبكة أو قيود الوصول لأنظمة زمامد التي تعالج بيانات حساسة أو خاضعة للتنظيم حتى يتم تطبيق الرقع
6. توثيق جميع أنشطة المعالجة والاحتفاظ بالأدلة لمتطلبات الامتثال التنظيمي والمراجعة