ثغرة يوم الصفر في Cacti دون تصحيح ومع استغلال منشور تتيح تنفيذ الأوامر عن بُعد دون مصادقة



كُشف عن ثغرة يوم صفر في منصة المراقبة Cacti مع استغلال تجريبي منشور يتيح لمهاجم غير مصادَق تنفيذ أوامر عند تفعيل حساب الضيف. لا يوجد تصحيح حتى الآن ولم تُسجَّل هجمات.

- الثغرة حقن SQL مخزَّن في إعدادات عرض الرسوم البيانية لمستخدم الضيف، ما يسمح بتعديل الأوامر التي ينفذها الـ poller.
- يتطلب الاستغلال تفعيل حساب الضيف في Cacti دون الحاجة إلى بيانات اعتماد صالحة.
- اختُبر الاستغلال على Cacti Core 1.2.31، ومن غير الواضح ما إذا كانت الإصدارات الأقدم متأثرة.
- تعتمد الصلاحيات المكتسبة على الحساب الذي يشغّل خادم الويب والـ poller، وقد تكون محدودة وليست root.
- لم تُسجَّل هجمات استغلال حتى 27 نوفمبر، ولم يصدر تصحيح بعد.

كُشف علنًا عن ثغرة يوم صفر في Cacti، وهي أداة مفتوحة المصدر تُستخدم لمراقبة الخوادم والموجّهات والمبدّلات وجدران الحماية وغيرها من البنية التحتية للشبكات، وذلك مع نشر استغلال تجريبي فعّال. ويذكر الباحث الذي نشره أنه لم يبلغ مشروع Cacti بالثغرة قبل ذلك.

طبيعة الثغرة

تكمن المشكلة في ضعف التحقق من المدخلات. إذ يستطيع المهاجم حفظ عبارات SQL خبيثة ضمن تفضيلات عرض الرسوم البيانية لمستخدم الضيف. وعندما يعالج Cacti هذه التفضيلات تُنفَّذ العبارات، فيتمكن المهاجم من تعديل إعدادات الـ poller ليشغّل أوامر على نظام التشغيل. ويربط الاستغلال المنشور هذه الخطوات في أربعة طلبات HTTP دون الحاجة إلى بيانات اعتماد، لكنه يشترط تفعيل حساب الضيف.

وقد أظهر الباحث الحصول على صلاحيات root، بينما توضح watchTowr أن الصلاحيات الفعلية تعتمد على الحساب الذي يشغّل خادم الويب والـ poller، وهو غالبًا حساب محدود الصلاحيات. واختُبر الاستغلال على Cacti Core 1.2.31، ولا يُعرف وضع الإصدارات الأقدم.

أهمية الأمر

قد يحتفظ Cacti ببيانات اعتماد وعبارات مرور SNMP للأجهزة التي يراقبها، ما قد يجعل خادمًا مخترقًا منه بوابة إلى أنظمة أخرى في شبكة المؤسسة. ولم تُسجَّل هجمات استغلال حتى 27 نوفمبر، غير أن نشر الاستغلال علنًا يقلّص عادةً الوقت المتاح للاستعداد.

إجراءات مؤقتة

إلى حين صدور تصحيح، يُنصح المسؤولون بتعطيل حساب الضيف وحصر الوصول إلى واجهة الويب في الشبكات الموثوقة. كما ينبغي مراجعة إعدادات الـ poller بحثًا عن أوامر غير متوقعة، وفحص السجلات بحثًا عن تحذيرات تتعلق بقيم غير رقمية في إعدادات عرض الرسوم البيانية، إذ قد تدل على محاولة استغلال.

ما يجب فعله الآن

1. حصر جميع نسخ Cacti في البيئة، بما فيها التي تديرها فرق الشبكات والبنية التحتية، وتسجيل الإصدار المستخدم في كل منها.
2. تعطيل حساب الضيف في Cacti على جميع النسخ إلى حين صدور تصحيح من المطوّر.
3. حصر الوصول إلى واجهة الويب لـ Cacti في شبكات الإدارة الموثوقة فقط.
4. مراجعة إعدادات الـ poller بحثًا عن أوامر غير متوقعة، وفحص سجلات التطبيق بحثًا عن تحذيرات تخص قيمًا غير رقمية في إعدادات عرض الرسوم البيانية.
5. التعامل مع بيانات الاعتماد وعبارات مرور SNMP المخزنة في Cacti على أنها حساسة، والاستعداد لتغييرها عند الاشتباه بوقوع اختراق.
6. متابعة إصدار التصحيح من مشروع Cacti وجدولة تطبيقه عبر إجراءات إدارة التغيير فور صدوره.