# ثغرة صفرية غير مُصحَّحة في Cacti قد تتيح تنفيذ الأوامر عن بُعد عبر وصول الضيف




ظهرت تفاصيل ثغرة صفرية غير مُصحَّحة في أداة المراقبة المفتوحة المصدر Cacti. يشير إثبات مفهوم باسم 4HTTP2SHELL و4HTTP2ROOT إلى الوصول لتنفيذ الأوامر من جلسة غير موثَّقة، ولم يُسند رقم CVE بعد.

- تؤثر الثغرة في Cacti، أداة مراقبة الشبكات المفتوحة المصدر، وقد تؤدي إلى تنفيذ أوامر عن بُعد.
- يُتتبَّع إثبات المفهوم باسمي 4HTTP2SHELL و4HTTP2ROOT.
- لم يُسند معرّف CVE للثغرة حتى الآن.
- يصف الباحث مساراً من جلسة HTTP جديدة غير موثَّقة إلى تنفيذ الأوامر بصلاحيات خادم Cacti.
- يشير العنوان إلى أن الهجوم يتطلب أربعة طلبات HTTP فقط ويعتمد على وصول الضيف.

ظهرت تفاصيل ثغرة غير معروفة سابقاً في Cacti، وهي أداة مفتوحة المصدر تُستخدم لمراقبة الشبكات. وبحسب التقرير، يُظهر إثبات مفهوم أن تنفيذ الأوامر عن بُعد ممكن، ويُتتبَّع تحت الاسمين 4HTTP2SHELL و4HTTP2ROOT. ولم يُسند للثغرة معرّف CVE حتى الآن.

## ما يذكره التقرير

يصف الباحث مساراً يبدأ من جلسة HTTP جديدة غير موثَّقة وينتهي بتنفيذ أوامر بصلاحيات خادم Cacti. ويذكر العنوان أن ذلك يتم بأربعة طلبات HTTP فقط وأن وصول الضيف جزء من المسار. ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية، ولا يشير إلى تصحيح من المطوّر، لذا نتعامل مع الثغرة بوصفها غير مُصحَّحة في الوقت الحالي.

## لماذا يهم ذلك

تقع منصات المراقبة عادةً قريباً من قلب الشبكة وتملك رؤية واسعة على أنظمة كثيرة. وثغرة تتيح تنفيذ الأوامر دون مصادقة على خادم كهذا تستحق الاهتمام حتى قبل صدور رقم CVE. وعلى الجهات التي تشغّل Cacti، ومنها داخل شبكات الإدارة الداخلية، أن تتأكد من أماكن نشره وكيفية الوصول إليه.

ونظراً لمحدودية المعلومات، فالنهج العملي هو تقليل التعرّض الآن ومتابعة صدور تصحيح ومعرّف رسمي. وينبغي تجنب الجزم بالإصدارات المتأثرة إلى أن يعلنها المشروع أو نشرة موثوقة.

## ما يجب فعله الآن

1. حصر جميع نسخ Cacti، بما فيها الموجودة في شبكات الإدارة الداخلية وبيئات الاختبار.
2. حصر الوصول الشبكي إلى Cacti في أجهزة الإدارة فقط وإزالة أي تعرّض مباشر للإنترنت.
3. مراجعة تفعيل وصول الضيف وتعطيله حيث لا حاجة إليه.
4. مراقبة سجلات الويب والخادم بحثاً عن طلبات غير معتادة أو تنفيذ أوامر غير متوقع.
5. متابعة مشروع Cacti والنشرات الموثوقة لمعرفة صدور التصحيح ورقم CVE، والتخطيط لتطبيقه فور توفره.