CISA تضيف ثغرة Perforce Puppet الحرجة CVE-2026-115731 إلى قائمة الثغرات المستغلة



أضافت CISA ثغرة حرجة في Perforce Puppet برقم (CVSS 9.4) CVE-2026-115731 إلى كتالوج KEV بعد تقارير عن استغلالها فعليًا. على الجهات التي تشغّل Puppet مراجعة تعرّضها.

- أضافت CISA يوم الثلاثاء ثغرة Perforce Puppet إلى كتالوج الثغرات المستغلة المعروفة (KEV).
- تحمل الثغرة الرقم CVE-2026-115731 وتصنيف CVSS بدرجة 9.4.
- استندت CISA إلى تقارير عن استغلال فعلي للثغرة.
- Puppet منصة مؤسسية للبنية التحتية ككود وإدارة التهيئة.
- المقتطف المتاح من المصدر مبتور ولا يوضح نوع الثغرة بدقة ولا الإصدارات المتأثرة ولا الإصلاحات.

أضافت الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA) ثغرة حرجة في Perforce Puppet إلى كتالوج الثغرات المستغلة المعروفة (KEV)، مشيرة إلى تقارير عن استغلالها فعليًا.

ما المعروف حتى الآن

تحمل الثغرة الرقم **CVE-2026-115731** وتصنيف CVSS بدرجة 9.4. وPuppet منصة مؤسسية للبنية التحتية ككود وإدارة التهيئة. ويصف عنوان التقرير الأصلي المشكلة بأنها ثغرة تنفيذ تعليمات برمجية عن بُعد تؤثر في خوادم الإدارة المؤسسية.

لكن المقتطف الذي اطلعنا عليه مبتور، فلا يذكر السبب التقني ولا الإصدارات المتأثرة ولا الجهات المهاجمة ولا توفر تحديث أمني. لذلك لم نورد هذه التفاصيل.

أهمية الخبر

تملك خوادم إدارة التهيئة عادةً صلاحيات إدارية واسعة على الأنظمة التي تديرها. ووجود ثغرة حرجة مستغلة فعليًا في منصة كهذه يستدعي اهتمامًا عاجلاً، خصوصًا في البيئات المنظمة التي تخضع فيها إدارة التغيير والصلاحيات المميزة لرقابة دقيقة.

النهج المقترح

ينبغي للجهات أولاً التأكد من استخدام Puppet في أي جزء من بيئتها، بما في ذلك الشركات التابعة ومزودو الخدمة. وإن كان مستخدمًا، فعليها الرجوع إلى نشرة المورّد لمعرفة الإصدارات المتأثرة والإصلاحات، وإعطاء المعالجة أولوية وفق إجراءات إدارة الثغرات. وإلى حين ذلك، يُقيَّد الوصول الشبكي إلى خوادم Puppet وتُراجع بحثًا عن نشاط غير معتاد.

ما يجب فعله الآن

1. حصر جميع خوادم ووكلاء Puppet، بما في ذلك ما تديره الشركات التابعة والأطراف الخارجية.
2. مراجعة نشرة Perforce الخاصة بالثغرة CVE-2026-115731 لتحديد الإصدارات المتأثرة والإصلاحات المتاحة.
3. تطبيق التحديث أو إجراءات التخفيف من المورّد بصورة عاجلة، بدءًا بالخوادم المتاحة من الإنترنت أو عالية الصلاحيات.
4. حصر الوصول الشبكي إلى خوادم Puppet في شبكات الإدارة المعتمدة فقط.
5. مراجعة السجلات وتغييرات التهيئة على خوادم Puppet بحثًا عن نشاط غير متوقع، وتصعيد أي ملاحظات عبر إجراءات الاستجابة للحوادث.