ثغرة Java4Shell (CVE-2026-114938): خطر تنفيذ تعليمات برمجية دون مصادقة في Jira وJenkins وKeycloak



كشفت شركة Calif عن ثغرة Java4Shell في Java تتيح لمهاجمين دون حساب تنفيذ تعليمات برمجية على Jira وJenkins وKeycloak وثلاثة تطبيقات أخرى، وتمس Java 17.0.6 وما بعدها على معالجات x86-64 معينة.

- الثغرة مسجلة برقم CVE-2026-114938 وتُعرف باسم Java4Shell.
- يستطيع مهاجم لا يملك حساباً تنفيذ تعليماته البرمجية على التطبيقات المتأثرة.
- من التطبيقات المذكورة Jira وJenkins وKeycloak، إضافة إلى ثلاثة أخرى لم يوردها المقتطف.
- الثغرة موجودة في Java 17.0.6 وما بعده.
- لا يعمل الشيفرة المعيبة إلا على معالجات Intel وAMD بمعمارية x86-64 التي تدعم ميزة

.AVX-512 VBMI

كشفت شركة الأبحاث الأمنية Calif هذا الأسبوع عن ثغرة في Java أطلقت عليها اسم Java4Shell، وهي مسجلة برقم CVE-2026-114938. ووفق تقرير The Hacker News، قد تتيح الثغرة لمهاجم لا يملك أي حساب تنفيذ تعليماته البرمجية على Jira وJenkins وKeycloak وثلاثة تطبيقات أخرى واسعة الاستخدام.

من المتأثر

الثغرة موجودة في Java 17.0.6 وما بعده. ولا يعمل المسار المعيب إلا على معالجات x86-64 من Intel وAMD التي تدعم ميزة AVX-512 VBMI. أي أن التعرض يعتمد على إصدار Java وعلى العتاد معاً، فلن تتأثر كل البيئات بالطريقة نفسها.

لم يذكر المقتطف أسماء التطبيقات الثلاثة الأخرى، ولم يتطرق إلى توفر التصحيحات أو الإصدارات المعالجة أو وجود استغلال فعلي. ينبغي مراجعة التقرير الأصلي وقنوات الموردين لمعرفة هذه التفاصيل.

الخطوات المقترحة

تقع هذه المنتجات غالباً في بيئات التطوير والهوية وسلاسل النشر، لذا تستحق ثغرة تنفيذ التعليمات قبل المصادقة اهتماماً عاجلًا ومتزناً. ابدأوا بحصر أماكن تشغيل إصدارات Java المتأثرة، ثم تحققوا من دعم معالجات الخوادم للميزة المذكورة. وأعطوا الأولوية للنسخ المكشوفة على الإنترنت وتلك التي تحتفظ بأسرار أو بيانات اعتماد.

إلى حين تأكيد إرشادات الموردين، قلّلوا التعرض بتقييد الوصول الشبكي إلى هذه الأنظمة ومراقبة أي نشاط غير معتاد عليها.

ما يجب فعله الآن

1. حصر بيئات Java بالإصدار 17.0.6 أو أحدث في Jira وJenkins وKeycloak وسائر التطبيقات المعتمدة على Java.
2. التحقق من كون معالجات الخوادم من Intel أو AMD بمعمارية x86-64 وتدعم AVX-512 VBMI لتحديد أولويات المعالجة.
3. تقييد الوصول الشبكي إلى الأنظمة المتأثرة، خاصة المكشوفة على الإنترنت، إلى حين تأكيد إرشادات الموردين.
4. متابعة نشرات الموردين وشركة Calif لمعرفة التصحيحات والإصدارات المعالجة وقائمة التطبيقات كاملة.
5. مراجعة السجلات والمراقبة على خوادم Jenkins وKeycloak بحثاً عن نشاط غير معتاد في العمليات أو الوصول.