CERT-EU: ثغرة عالية الخطورة في OpenJDK برقم CVE-2026-114938 قد تتيح تنفيذ التعليمات عن بُعد دون مصادقة



أصدرت Oracle ومشروع OpenJDK في 17 نوفمبر 2026 إصلاحات للثغرة CVE-2026-114938 (CVSS 8.1)، وهي تلف في الذاكرة قد يسبب حجب الخدمة وأحيانًا تنفيذ تعليمات عن بُعد دون مصادقة. وينصح CERT-EU بإعطاء الأولوية للتطبيقات المواجهة للإنترنت.

- الثغرة CVE-2026-114938 بدرجة CVSS تبلغ 8.1، وهي تلف في الذاكرة داخل OpenJDK.
- يتطلب الاستغلال معالج x86-64 بميزات AVX-512 وBMI2 محددة، وتفعيل دالة Base64 المدمجة، ووصول بيانات Base64 يتحكم بها المهاجم إلى أداة فك الترميز.
- أنظمة ARM64 غير متأثرة.
- تتوفر إصلاحات لإصدارات Java SE / OpenJDK 8 (نسخ الأداء) و17 و21 و25 و27، بينما تصدر التوزيعات الأخرى لـOpenJDK إصلاحاتها وفق جداولها.

- يمكن كحل مؤقت تعطيل الدالة المدمجة أو AVX-512 ثم إعادة تشغيل JVM.

في 17 نوفمبر 2026 أصدرت Oracle ومشروع OpenJDK إصلاحات للثغرة CVE-2026-114938، وهي ثغرة تلف في الذاكرة داخل OpenJDK. يصنفها CERT-EU عالية الخطورة (CVSS 8.1)، وقد تؤدي إلى حجب الخدمة، وفي ظروف معينة إلى تنفيذ تعليمات عن بُعد دون مصادقة.

من المعرّض للخطر

يتطلب الاستغلال اجتماع عدة شروط. يجب أن تعمل JVM على معالج x86-64 يدعم avx512f وavx512bw (Intel Xeon Ice Lake وavx512vbmi bmi2 أو أحدث، AMD Zen 4 أو أحدث). ويجب أن تكون دالة Base64 المدمجة مفعّلة، وهو الوضع الافتراضي على هذه المعالجات. كما يجب أن تصل بيانات Base64 يتحكم بها المهاجم إلى أداة فك الترميز، مثل مصادقة HTTP Basic أو JWT أو رسائل SAML أو ملفات تعريف الارتباط أو بيانات TLS. أنظمة ARM64 غير متأثرة.

تشمل المنتجات المتأثرة Oracle Java SE 8 نسخ الأداء (8u511-perf)، وJava SE / OpenJDK 17 (من 17.0.6 إلى 17.0.21)، و21 (حتى 21.0.13)، و25 (حتى 25.0.5)، و27 (حتى 27.0.1)، وOracle GraalVM for JDK 17 و21. كما تتأثر توزيعات مثل Eclipse Temurin وAmazon Corretto وAzul Zulu وMicrosoft Build of OpenJDK وBellSoft Liberica وSAP SapMachine وRed Hat build of OpenJDK، وتصدر إصلاحاتها وفق جداولها الخاصة. وتعمل على هذه المنصات تطبيقات مثل Keycloak وبعض منتجات Atlassian وJFrog Artifactory، وتبقى المنتجات التي تضم بيئة Java خاصة بها متأثرة إلى حين صدور تحديث من مورّدها.

ما العمل

يوصي CERT-EU بتحديث الإصدارات المتأثرة مع إعطاء الأولوية للتطبيقات المواجهة للإنترنت، ثم إعادة تشغيل جميع JVM. وإن تعذر التحديث الفوري يمكن تعطيل الدالة المدمجة بالخيار -- XX:+UnlockDiagnosticVMOptions XX:-UseBASE64Intrinsics، أو تعطيل AVX-512 بالخيار -XX:UseAVX=2 وقد يقلل ذلك الأداء. كلا الخيارين يتطلب إعادة تشغيل JVM.

ما يجب فعله الآن

1. حصر بيئات Java التشغيلية، بما فيها المضمّنة في منتجات الأطراف الثالثة، وتحديد الإصدارات المتأثرة.
2. تحديث تطبيقات Java المواجهة للإنترنت أولاً ثم إعادة تشغيل جميع JVM.
3. تحديد الخوادم التي تعمل بمعالجات x86-64 ذات ميزات AVX-512 وBMI2 المذكورة لضبط الأولويات.
4. عند تعذر التحديث فورًا، تطبيق خيار JVM لتعطيل الدالة المدمجة أو AVX-512 والتحقق من الإعداد.
5. متابعة نشرات المورّدين مثل Temurin وCorretto وZulu وRed Hat، ومطالبة موردي البيئات المضمّنة بمواعيد التحديث.
6. توثيق المعالجة ضمن عملية إدارة الثغرات والتحديثات.