Java4Shell (CVE-2026-114938): ثغرة حرجة في OpenJDK تتيح تنفيذ الشيفرة عن بُعد



ثغرة حرجة في مفكك Base64 ضمن OpenJDK (CVE-2026-114938) قد تؤدي إلى تنفيذ الشيفرة عن بُعد في تطبيقات مؤسسية شائعة. أصدرت Oracle التحديثات، وتوجد حلول مؤقتة.

- الثغرة CVE-2026-114938 خلل في تلف الذاكرة داخل مفكك Base64 المسرَّع بالعتاد في OpenJDK بدءًا من الإصدار 17.0.6، وفي توزيعات Java المبنية على الشيفرة نفسها.
- صنّفها باحثو Calif بدرجة 9.2 وفق CVSS 4.0، بينما صنّفتها Oracle بدرجة 8.1 (عالية) وفق CVSS 3.1.
- نجح الباحثون في تنفيذ شيفرة عن بُعد دون مصادقة ضد Keycloak وJira وConfluence وArtifactory وJenkins وPingFederate بإعداداتها الافتراضية.
- يتطلب الاستغلال مسارًا خاصًا بكل تطبيق لإيصال البيانات إلى المفكك، ومعالجات x86-64 تدعم AVX-512 VBMI، ولا يوجد استغلال شامل.

- أصدرت Oracle الإصلاح في 17 نوفمبر؛ وتوجد شيفرة إثبات مفهوم لتلف الذاكرة منشورة، دون نشر أدوات الاستغلال الجاهزة.

كُشف عن ثغرة حرجة في OpenJDK أُطلق عليها اسم Java4Shell وتحمل الرقم CVE-2026-114938. ولأن تطبيقات كثيرة غير مترابطة تعتمد بيئة Java نفسها، فإن أي خلل في مكوّن أساسي قد يطال طيفًا واسعًا من الأنظمة المؤسسية.

ما الذي يتأثر

تتمثل الثغرة في خلل لتلف الذاكرة داخل دالة فك ترميز Base64 المسرَّعة بالعتاد. فبيانات Base64 مصمَّمة خصيصًا قد تكتب فوق أجزاء من ذاكرة Java، ما قد يكشف معلومات حساسة أو يتيح تنفيذ الشيفرة عن بُعد. وتشمل الثغرة OpenJDK بدءًا من 17.0.6 والتوزيعات المبنية على الشيفرة نفسها، ومنها Oracle Java SE وAmazon Corretto وEclipse Temurin وMicrosoft Build of OpenJDK وAzul Zulu وRed Hat OpenJDK.

وأظهرت شركة Calif التي كشفت الثغرة تنفيذ شيفرة دون مصادقة ضد Keycloak وAtlassian Jira وConfluence وJenkins وJFrog Artifactory وPingFederate بإعداداتها الافتراضية، وتنفيذًا بعد المصادقة ضد Apache Kafka وApache Solr وElasticsearch وGerrit وSpinnaker.

حدود مهمة

لا يوجد استغلال شامل؛ إذ يحتاج المهاجم إلى طريقة خاصة بكل تطبيق لإيصال البيانات الخبيثة إلى المفكك، كما أن الدالة المعرّضة لا تُستخدم إلا على معالجات x86-64 التي تدعم AVX-512 VBMI. وتتوفر شيفرة إثبات مفهوم تُظهر تلف الذاكرة، أما أدوات الاستغلال الجاهزة فلم تُنشر.

الإصلاح والحلول المؤقتة

أصدرت Oracle التحديثات في 17 نوفمبر ضمن تحديثها الأمني الحرج لشهر نوفمبر، وتوصي العملاء بتطبيقها سريعًا. وإن تعذّر التحديث الفوري، تقترح Calif تشغيل Java بالخيار -XX:-UseBASE64Intrinsics، أو -XX:UseAVX=2 على أنظمة x86-64 لتعطيل تعليمات AVX-512. وهذه إجراءات مؤقتة، ويبقى تحديث بيئة Java هو الحل.

ما يجب فعله الآن

1. حصر جميع بيئات Java والتطبيقات المبنية عليها (ومنها Jenkins وJira وConfluence وKeycloak وArtifactory وPingFederate) وتحديد ما يعمل على OpenJDK 17.0.6 أو أحدث.
2. تطبيق تحديثات Oracle لشهر نوفمبر أو التحديث المقابل من مورّد توزيعة Java، مع أولوية للأنظمة المكشوفة للإنترنت وأنظمة الهوية.
3. عند تأجيل التحديث، تطبيق -XX:-UseBASE64Intrinsics أو -XX:UseAVX=2 كإجراء مؤقت وتوثيقه كاستثناء له مسؤول وتاريخ انتهاء.
4. تحديد الخوادم التي تعمل بمعالجات x86-64 الداعمة لـ AVX-512 VBMI لتركيز الأولويات.
5. تعزيز مراقبة تطبيقات Java المكشوفة بحثًا عن مدخلات Base64 غير معتادة ونشاط عمليات غير

متوقع، وإدارة التحديث وفق إجراءات التغيير وإدارة الثغرات.