CISA تحث على التصحيح الفوري لثغرة Java الحرجة CVE-2026-114938 المعروفة بـ "Java4Shell"



تحث CISA الجهات على تصحيح الثغرة الحرجة CVE-2026-114938 في HotSpot JVM لمعمارية x86-64، والتي قد تتيح تنفيذ تعليمات عن بُعد دون مصادقة عبر مدخلات Base64 مصممة خصيصاً.

- الثغرة CVE-2026-114938 المعروفة بـ "Java4Shell" خلل حرج في تلف الذاكرة داخل مفكك Base64 في HotSpot JVM لمعمارية x86-64.
- قد تؤدي مدخلات Base64 مصممة خصيصاً إلى انهيار JVM وتنفيذ تعليمات عن بُعد دون مصادقة.
- قد تكون Java مضمّنة في تطبيقات الأطراف الثالثة وصور الحاويات والأجهزة، وقد لا تظهر كبند مستقل في جرد البرمجيات.
- تُعطى الأولوية للأنظمة المكشوفة على الإنترنت، مع ضوابط تعويضية عند تعذر التصحيح الفوري.

- نشرت Oracle نشرة أمنية (Critical Security Patch Update – November 2026) توضح المنتجات والإصدارات المتأثرة.

أصدرت CISA تنبيهاً تحث فيه الجهات على تصحيح ثغرة حرجة في Oracle Java تحمل الرقم CVE-2026-114938 وتُعرف باسم "Java4Shell"، وقد شارك في التنبيه المركز الكندي للأمن السيبراني.

ما الذي تأثر

تتمثل الثغرة في خلل تلف ذاكرة في مفكك Base64 ضمن HotSpot Java Virtual Machine لمعمارية x86-64، وهو جزء من Java Development Kit. وبحسب CISA فإن مدخلات Base64 مصممة خصيصاً قد تتسبب في انهيار JVM وتتيح تنفيذ تعليمات عن بُعد دون مصادقة.

وتشير CISA إلى صعوبة رصد بيئات Java، إذ قد تكون مضمّنة في تطبيقات الأطراف الثالثة أو في صور الحاويات والأجهزة، وقد لا تظهر كبنود مستقلة في جرد البرمجيات.

ما توصي به CISA

ينبغي للجهات أولًا تحديد تثبيتات Java المتأثرة، ثم تطبيق تصحيحات Oracle والموردين فور توفرها، بدءاً بالأنظمة المكشوفة على الإنترنت. وتوضح نشرة Oracle بعنوان Critical Security Patch Update – November 2026 المنتجات والإصدارات المتأثرة.

وإذا تعذر التصحيح الفوري، تقترح CISA ضوابط تعويضية مؤقتة، منها تقييد مدخلات Base64 والتحقق منها عند حدود التطبيق، وفرض حدود لحجم المدخلات، والحد من الوصول غير المصادق. كما ينبغي مراقبة مؤشرات النشاط المشبوه، ومنها بيئات التشغيل غير المصرح بها وانهيارات JVM غير المتوقعة وعمليات Java المشبوهة.

الخطوة العملية التالية

قد يكون الجزء الأصعب لدى معظم المؤسسات هو العثور على كل نسخة من Java، بما فيها المضمّنة في منتجات الموردين. وبدء هذا الحصر الآن بالتوازي مع مراجعة نشرة Oracle يختصر الوقت اللازم للتصحيح عند توفر الإصلاحات لكل نظام.

ما يجب فعله الآن

1. حصر جميع حزم JDK وبيئات تشغيل Java، بما فيها المضمّنة في تطبيقات الأطراف الثالثة وصور الحاويات والأجهزة.
2. مراجعة نشرة Oracle الأمنية لشهر نوفمبر 2026 لتأكيد المنتجات والإصدارات المتأثرة.
3. تصحيح أنظمة Java المكشوفة على الإنترنت أولًا ثم بقية الأنظمة فور توفر تصحيحات Oracle والموردين.
4. عند تأخر التصحيح، تقييد مدخلات Base64 والتحقق منها عند حدود التطبيق، وتحديد حجم المدخلات، والحد من الوصول غير المصادق.
5. مراقبة بيئات التشغيل غير المصرح بها وانهيارات JVM غير المتوقعة وعمليات Java المشبوهة.

6. مطالبة موردي البرمجيات والأجهزة بتأكيد ما إذا كانت منتجاتهم تتضمن إصدارات Java متأثرة.