اختراق حزمة Tensorlake على npm ضمن هجوم سلسلة توريد مرتبط بالدودة Shai-Hulud



أُصيب الإصدار 0.5.144 من حزمة tensorlake على npm ببرمجية خبيثة مشفّرة تسرق بيانات الاعتماد والأسرار. ينبغي للفرق المستخدمة للحزمة مراجعة اعتمادياتها.

- تعرّضت حزمة tensorlake على npm، وهي حزمة TypeScript SDK لتطبيقات Tensorlake وبيئات العزل والخدمات السحابية، للاختراق.
- الإصدار الخبيث هو 0.5.144.
- الحادثة مرتبطة بهجوم سلسلة توريد يُعرف باسم Shai-Hulud / ChainDrop.
- وفق شركة Socket، تجمع البرمجية الخبيثة بيانات الاعتماد وتسرّب الأسرار وتثبّت بقاءها وتنفّذ شيفرة تصلها عن بُعد.

ما الذي حدث

تعرّضت حزمة "tensorlake" على npm، وهي حزمة تطوير برمجية بلغة TypeScript لتطبيقات Tensorlake وبيئات العزل والخدمات السحابية، للاختراق ضمن هجوم سلسلة توريد يُعرف باسم Shai-Hulud / ChainDrop. والإصدار المتأثر هو 0.5.144.

وبحسب شركة Socket، يحتوي الإصدار الخبيث على برمجية خبيثة مشفّرة تجمع بيانات الاعتماد وتسرّب الأسرار وتثبّت بقاءها في الجهاز وتنفّذ شيفرة يوفّرها المهاجم عن بُعد.

لماذا يهم ذلك

تُثبَّت حزم كهذه عادةً على أجهزة المطورين وفي مسارات البناء، حيث تتوافر غالباً الرموز والمفاتيح وبيانات الاعتماد السحابية. ولذلك قد يتجاوز أثر برمجية تسرق الأسرار وتحافظ على موطئ قدم الجهاز الذي ثُبّتت عليه. ولا يذكر المصدر عدد عمليات التثبيت المتأثرة ولا كيفية اختراق الحزمة، لذا لا ينبغي افتراض السلامة دون تحقق.

الخطوات التالية

ابدأوا بالتحقق مما إذا كان الإصدار 0.5.144 قد ثُبّت في أي من بيئاتكم. وإن حدث ذلك، فاعتبروا الجهاز وكل الأسرار التي يمكنه الوصول إليها مكشوفة وأعيدوا تدويرها. وتبيّن الإجراءات أدناه ترتيباً عملياً للعمل.

ما يجب فعله الآن

1. ابحثوا في ملفات القفل والمستودعات وسجلات البناء عن حزمة tensorlake بالإصدار 0.5.144.
2. عند العثور عليها، اعزلوا الجهاز أو منفّذ البناء المتأثر واعتبروا بيانات الاعتماد والرموز والمفاتيح التي يصل إليها مخترقة.
3. أعيدوا تدوير الأسرار المكشوفة، ومنها اعتمادات السحابة وCI/CD، وراجعوا استخدامها للكشف عن أي وصول غير مصرّح به.
4. أزيلوا الإصدار الخبيث، وثبّتوا إصداراً سليماً موثوقاً، وافحصوا الأنظمة المتأثرة بحثاً عن آليات بقاء.
5. راجعوا ضوابط استخدام الحزم الخارجية، مثل تثبيت الإصدارات وتأخير اعتماد الإصدارات الجديدة.