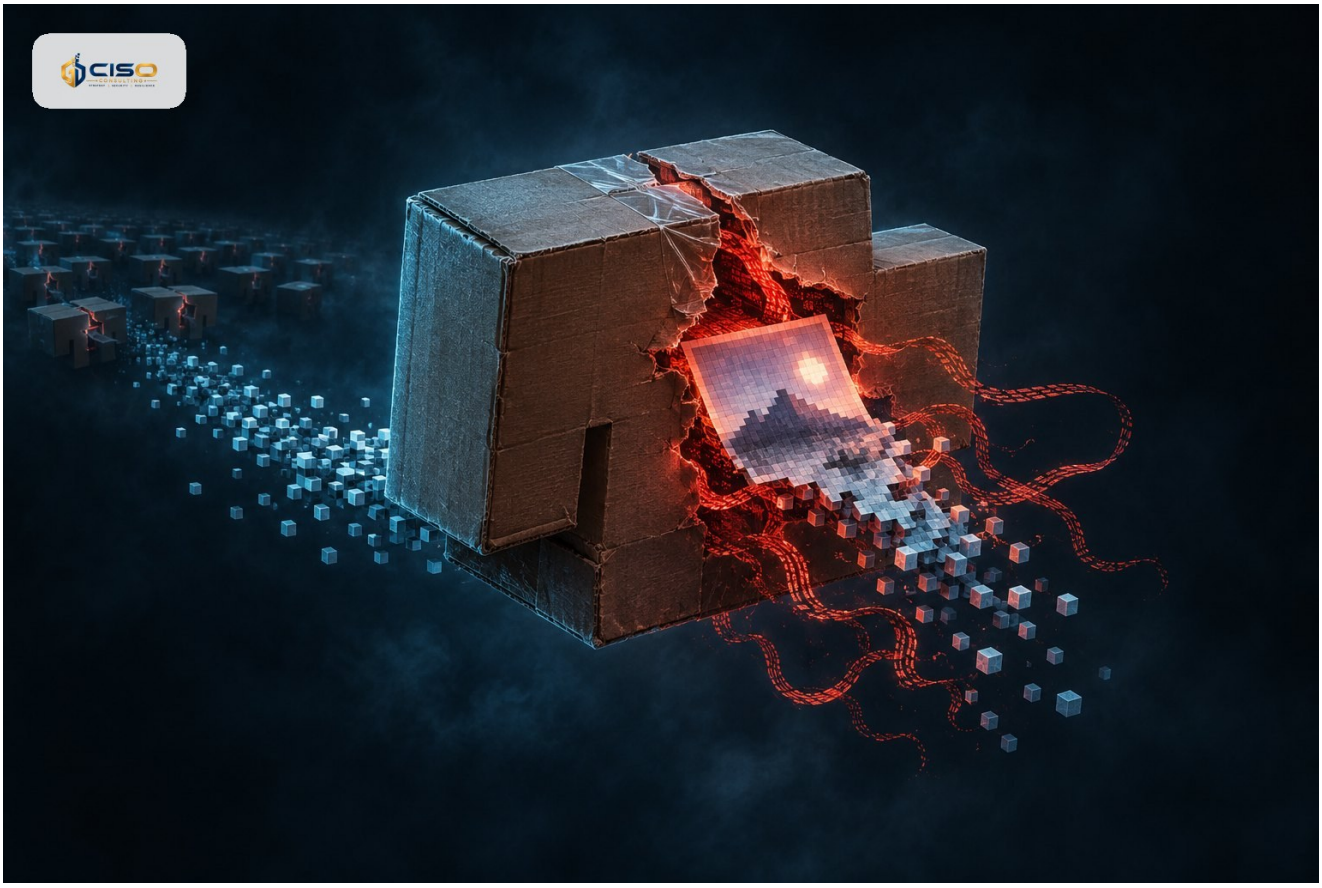
حزمة npm خبيثة باسم imgdecode ضمن حملة MALFEX لسلسلة التوريد البرمجية



اكتشف باحثون حزمة npm خبيثة باسم imgdecode ضمن حملة MALFEX. رُفعت في 30 سبتمبر 2026 وسُجّل لها 979 تنزيلًا، وكانت ما تزال متاحة وقت النشر.

- الحزمة imgdecode جزء من حملة سلسلة توريد برمجية تحمل اسم MALFEX.
- رفعها إلى npm مستخدم باسم malfexteste8 بتاريخ 30 سبتمبر 2026.
- بلغ عدد تنزيلاتها 979 مرة وكانت ما تزال متاحة وقت إعداد التقرير.
- يشير عنوان المصدر إلى أنها تخفي محمّل شيفرة (shellcode) داخل إضافة أصلية لنظام Windows.

حدّد باحثو الأمن السيبراني حزمة npm خبيثة باسم imgdecode ضمن MALFEX، وهي حملة هجوم على سلسلة التوريد البرمجية أُعلن عنها مؤخراً.

ما هو معروف

نُشرت الحزمة في سجل npm بتاريخ 30 سبتمبر 2026 عبر حساب باسم malfexteste8. وحتى وقت إعداد التقرير كانت قد نُزّلت 979 مرة وما زالت متاحة للتنزيل. ووفق عنوان المصدر، فإنها تُخفي محمّل شيفرة (shellcode) داخل إضافة أصلية (native addon) لنظام Windows.

لا يوضح المقتطف المتاح لنا سلوك المحمّل ولا الحمولة ولا النطاق الأوسع لحملة MALFEX، لذلك لا نُخمّن في هذه النقاط.

أهمية الخبر

تعتمد المؤسسات التي تطوّر تطبيقات JavaScript وNode.jsg على حزم طرف ثالث بشكل اعتيادي. وقد تنفّذ الحزمة التي تبدو أداة عادية لكنها تضم إضافة أصلية شيفرة على أجهزة المطورين أو خوادم البناء، ولذلك يستحق فحص ما يدخل من تبعيات المراجعة حتى دون الاشتباه بحادثة.

النهج المقترح

ينبغي للفرق البحث عن اسم الحزمة في المستودعات وملفات القفل وسجلات البناء، واعتبار أي تطابق اختراقاً محتملًا للجهاز الذي ثبّتها. ويُفضّل الرجوع إلى تقرير الباحثين الأصلي للاطلاع على التفاصيل التقنية قبل اعتماد أي استجابة نهائية.

ما يجب فعله الآن

1. البحث في المستودعات وملفات القفل وسجلات CI/CD عن imgdecode وعن أي تثبيت من المستخدم malfexteste8.
2. عند العثور على تطابق، عزل جهاز المطور أو خادم البناء المتأثر وبدء معالجة الحادثة بما يشمل تدوير بيانات الاعتماد.
3. مراجعة تقرير الباحثين الأصلي للاطلاع على مؤشرات الاختراق قبل إغلاق التحقيق.
4. حصر تثبيت حزم npm في سجل داخلي معتمد أو قائمة سماح بحزم تمت مراجعتها.
5. إضافة مراجعة التبعيات التي تتضمن إضافات أصلية إلى إجراءات التطوير الآمن.