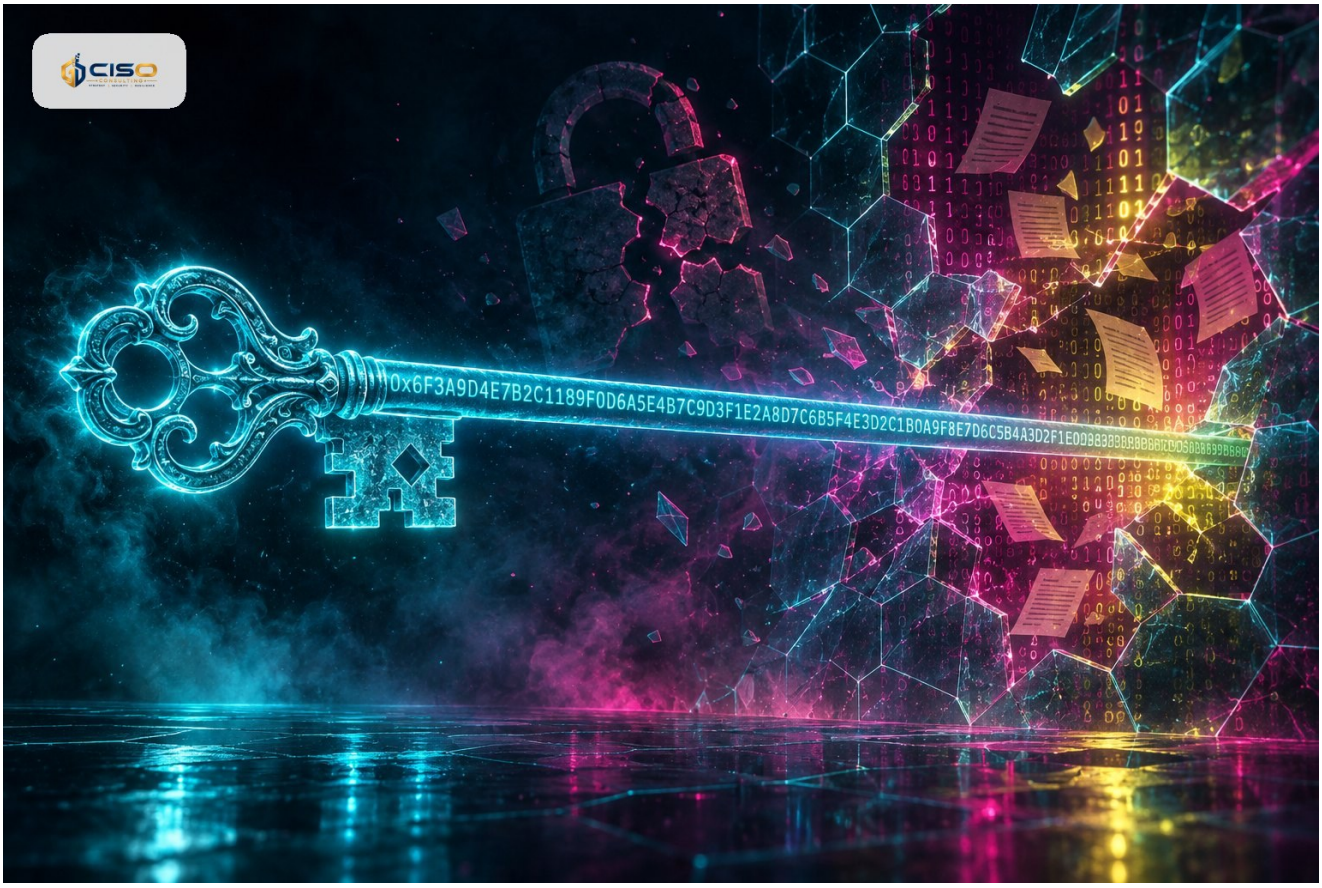
GnuPG تحذّر من ثغرة حرجة في GPGME يمكن استغلالها عبر مفاتيح OpenPGP خبيثة



أعلن مشروع GnuPG عن ثغرة حرجة في الذاكرة بمكتبة GPGME (CVE-2026-129975) تُفعَّل بمفتاح OpenPGP يحمل معرّف مستخدم طويلاً بشكل غير معتاد، وقد تكشف بيانات التطبيقات. الإصدار 2.3.0 يتضمن الإصلاح.

- الثغرة مسجلة برقم CVE-2026-129975 وتوصف بأنها حرجة.
- مفتاح OpenPGP خبيث بمعرّف مستخدم طويل بشكل غير معتاد قادر على تفعيل خلل الذاكرة.
- قد تُستغل الثغرة لسرقة بيانات من التطبيقات المتأثرة.
- تتأثر كل البرمجيات التي تستخدم GPGME قبل الإصدار 2.3.0.
- أصدر مشروع GnuPG نسخًا مصححة.

حذّر مشروع GnuPG من ثغرة حرجة في الذاكرة داخل مكتبة GPGME، وهي المكتبة القياسية التي تعتمد عليها البرامج للتعامل مع GnuPG. وقد سُجلت الثغرة برقم CVE-2026-129975.

ما الذي يتأثر

يمكن تفعيل الثغرة عبر مفتاح OpenPGP خبيث يحمل معرّف مستخدم طويلاً بشكل غير معتاد. ووفق المشروع، قد يُستخدم ذلك لسرقة بيانات من التطبيقات التي تعتمد على المكتبة. وتشمل الثغرة كل البرمجيات التي تستخدم GPGME في إصدارات سابقة للإصدار 2.3.0. وقد أصدر المشروع نسخًا مصححة.

ولأن GPGME مكتبة وليست منتجًا مستقلاً، قد لا يكون التعرض واضحًا؛ فالتطبيقات التي تتولى التشفير أو التوقيع أو استيراد المفاتيح عبر GnuPG قد تتضمنها مباشرة أو كتبعية.

الخطوات التالية

لا يذكر المصدر وجود استغلال فعلي، لذا تكون الأولوية للحصر المنظم والتحديث لا للإجراءات الطارئة. ينبغي للجهات تحديد مواضع استخدام GPGME، والترقية إلى الإصدار 2.3.0 أو أحدث، والحذر من مفاتيح OpenPGP الواردة من مصادر غير موثوقة إلى حين اكتمال التحديث.

وإذا كان التطبيق يضم نسخته الخاصة من المكتبة، فغالبًا يعتمد الإصلاح على مورّد التطبيق، لذا يُنصح بطلب تأكيد موقفه كتابيًا.

ما يجب فعله الآن

1. حصر التطبيقات والخوادم والأدوات التي تستخدم GPGME أو GnuPG، بما فيها التبعيات غير المباشرة.
2. ترقية GPGME إلى الإصدار 2.3.0 أو أحدث، مع إعطاء الأولوية للأنظمة المواجهة للإنترنت والتي تعالج بيانات حساسة.
3. مطالبة مورّدي البرمجيات التي تضمّن GPGME بتأكيد تأثر منتجاتهم وموعد إصدار الإصلاحات.
4. تجنب استيراد مفاتيح OpenPGP من مصادر غير موثوقة إلى حين اكتمال التحديث.
5. توثيق الثغرة وإجراءات المعالجة ضمن عملية إدارة الثغرات.