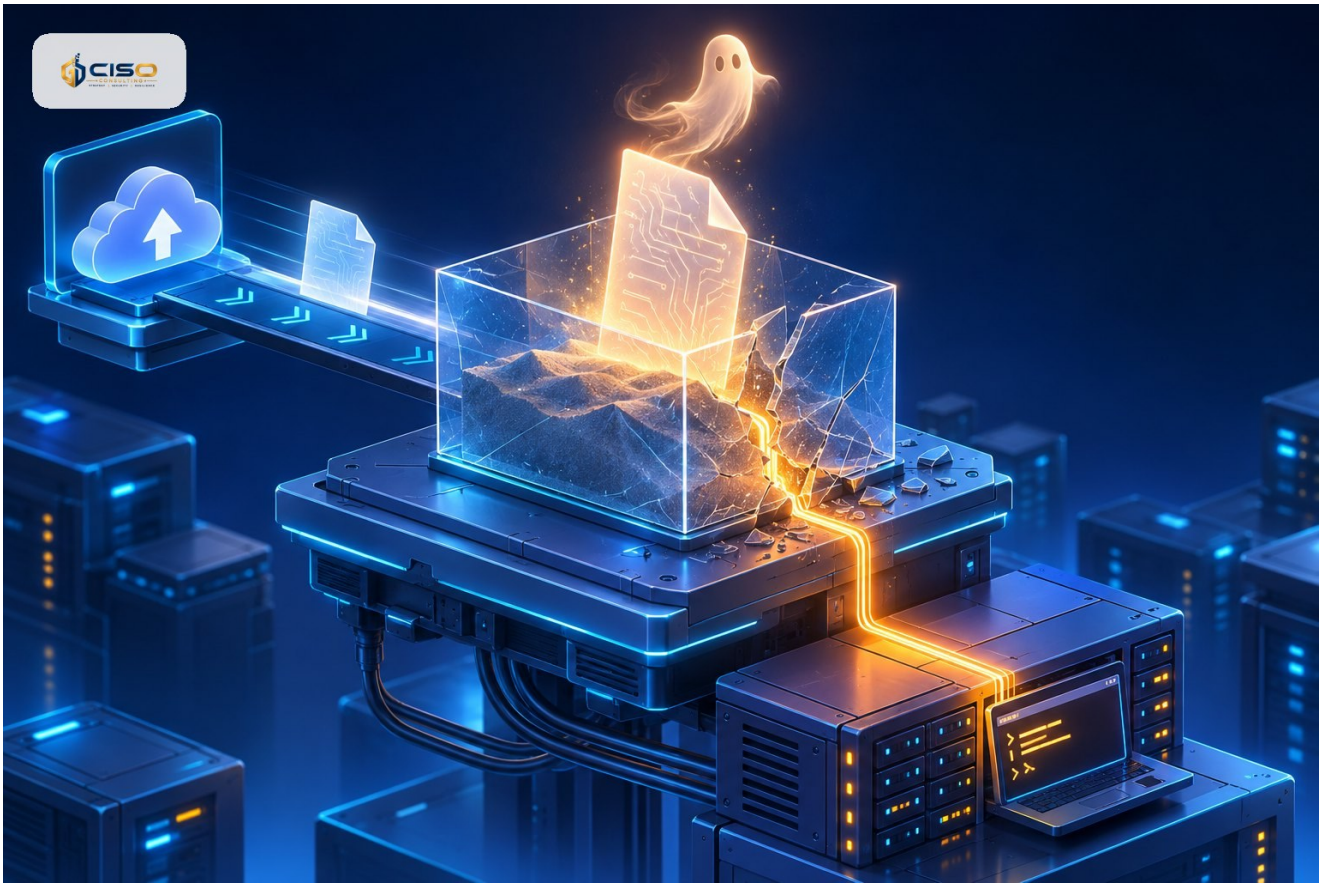
ثغرة مُصلحة في Ghostscript تتيح لملف مُعدّ تجاوز العزل وتنفيذ أوامر على الخادم



أظهر باحثو pwn.ai أن ثغرة مُصلحة في Ghostscript تسمح لملف مُعدّ بالخروج من بيئة العزل وتنفيذ أوامر على الخادم الذي يعالجه، عبر ميزات رفع الملفات في تطبيقات شائعة.

- تتيح الثغرة لملف مُعدّ الخروج من بيئة العزل الأمنية في Ghostscript.
- قد يؤدي ذلك إلى تنفيذ أوامر على الخادم الذي يعالج الملف.
- يُستخدم Ghostscript كثيرًا على خوادم Linux لتحويل ملفات PDF وPostScript والصور المرفوعة، وقد يحدث ذلك دون استدعاء مباشر من التطبيق.
- عرضت شركة pwn.ai الهجوم عبر ميزات رفع الملفات المعتادة.
- الثغرة مُصلحة، ولم يذكر المصدر رقم CVE ولا تفاصيل الإصدارات.

ما الذي عُرض

أظهرت شركة الأمن pwn.ai أن ثغرة في Ghostscript، أُصلحت الآن، تسمح لملف مُعدّ خصيصًا بالخروج من بيئة العزل الأمنية للبرنامج وتنفيذ أوامر على الخادم الذي يعالجه. واعتمد العرض على وظائف رفع الملفات المعتادة في تطبيقات شائعة.

لماذا يهم ذلك

يُعد Ghostscript المفسّر الذي تعتمد عليه خوادم Linux كثيرة لتحويل ملفات PDF وPostScript والصور المرفوعة إلى صيغ أخرى. وتستخدمه التطبيقات غالبًا بصورة غير مباشرة عبر مكتبات معالجة المستندات والصور، فقد تشغّله الجهات دون أن تختاره أو تعلم بوجوده. ولذلك قد تدخل في نطاق التعرّض أي خدمة تقبل ملفات من المستخدمين ثم تحوّلها أو تعرض معاينة لها.

لا يذكر المقتطف رقم CVE ولا أرقام الإصدارات المتأثرة ولا أسماء التطبيقات التي اختُبرت، لذا ينبغي التحقق من هذه التفاصيل في البحث الأصلي وملاحظات الإصدار الصادرة عن المورّد.

الخطوة التالية

بما أن الثغرة مُصلحة، فالأولوية هي تحديد أماكن تثبيت Ghostscript والتأكد من وجود الإصدار المُصلح. كما ينبغي مراجعة عزل الخدمات التي تعالج الملفات المرفوعة، إذ يقلّ أثر تجاوز العزل كثيرًا عندما تكون صلاحيات الخدمة المحوَّلة واتصالاتها بالشبكة محدودة.

ما يجب فعله الآن

1. حصر الخوادم والحاويات المثبّت عليها Ghostscript، بما في ذلك النسخ التي تأتي كاعتمادية لأدوات معالجة المستندات أو الصور.
2. تطبيق إصدار Ghostscript المُصلح من المورّد والتحقق من رقم الإصدار بعد التحديث.
3. تحديد التطبيقات التي تحوّل أو تعاين ملفات PDF وPostScript والصور المرفوعة من المستخدمين ومراجعتها أولاً.
4. تشغيل خدمات تحويل الملفات بأدنى الصلاحيات مع تقييد الاتصالات الصادرة وفصلها عن الأنظمة الأساسية.
5. مراجعة سجلات خوادم معالجة الملفات بحثًا عن عمليات فرعية غير متوقعة أو اتصالات صادرة غير معتادة.