

نشر برمجية استغلال علنية لثغرة في AnyDesk على لينكس تتيح صلاحيات الجذر دون مصادقة



نشر باحثون برمجية استغلال عاملة لثغرة تنفيذ تعليمات عن بُعد قبل المصادقة في AnyDesk على لينكس تمنح صلاحيات الجذر. أصلحتها الشركة في الإصدار 8.0.3 في يونيو ووصفتها بأنها خلل يسبب انهيار البرنامج.

- أصبحت برمجية استغلال عاملة للثغرة متاحة علناً.
- تتيح الثغرة تنفيذ تعليمات عن بُعد بصلاحيات الجذر قبل أن يوافق أحد على الاتصال.
- صدر الإصلاح في الإصدار 8.0.3 من AnyDesk في يونيو.
- وصف سجل التغييرات الإصلاح بأنه خلل قد يسبب انهيار البرنامج، ولم يُخصَّص رقم CVE.
- قد تكون الفرق التي تعتمد على صياغة سجل التغييرات أو تغذيات CVE قد فاتها هذا الإصلاح.

نشر باحثون أمنيون برمجية استغلال كاملة وعامة لثغرة في AnyDesk على نظام لينكس. الثغرة من نوع تنفيذ تعليمات عن بُعد قبل المصادقة، أي أن المهاجم لا يحتاج إلى بيانات اعتماد صالحة، وتمنحه صلاحيات الجذر قبل أن يوافق أي مستخدم على الاتصال الوارد.

ما هو معروف

عاجلت AnyDesk الثغرة في الإصدار 8.0.3 في يونيو، غير أن سجل التغييرات وصف التعديل بأنه إصلاح لخلل قد يتسبب في انهيار البرنامج فقط. ولم يُخصّص رقم CVE، ولم يصاحب الإصدار نشرة أمنية بحسب المصدر. ولا يذكر المصدر ما إذا كانت الثغرة قد استُغلت فعليًا.

أهمية الأمر

لأن الإصلاح لم يُصنّف تحديًا أمنيًا، فقد لا تعامل الجهات التي تحدد أولويات التحديث وفق تغذيات CVE أو صياغة النشرات الإصدار 8.0.3 على أنه عاجل. ومع توفر برمجية استغلال علنية، ينبغي اعتبار أي جهاز لينكس يعمل بإصدار أقدم من AnyDesk معرضًا لاختراق بصلاحيات الجذر.

النهج الموصى به

الأولوية هي حصر كل أجهزة لينكس المثبت عليها AnyDesk، والتحقق من إصدارها، ثم تحديثها أو إزالة البرنامج. وإذا لم تكن أدوات الوصول عن بُعد ضرورية على الخوادم فإزالتها هي الخيار الأقل مخاطرة. وتُعامل أي جلسات AnyDesk غير مفسّرة أو عمليات غير متوقعة على الأجهزة المتأثرة بوصفها حالات تستدعي التحقيق.

ما يجب فعله الآن

1. حصر جميع أجهزة لينكس المثبت عليها AnyDesk وتسجيل إصداراتها.
2. تحديث AnyDesk إلى الإصدار 8.0.3 أو أحدث، أو إزالته حيث لا حاجة إليه.
3. تقييد الاتصالات الواردة إلى AnyDesk على خوادم لينكس والأنظمة الحرجة إلى حين التحديث.
4. مراجعة السجلات على الأجهزة المتأثرة بحثًا عن جلسات AnyDesk غير متوقعة أو عمليات جديدة بصلاحيات الجذر.
5. إدراج ملاحظات إصدار المورد، وليس تغذيات CVE وحدها، ضمن عملية متابعة التحديثات لأدوات الوصول عن بُعد.