Tailscale تصدر الإصدار 1.104.4 لمعالجة ثغرات في SSH قد تتيح الوصول إلى خدمات خاصة بالمستخدم root على خوادم أخرى



أصدرت Tailscale الإصدار 1.104.4 لمعالجة ثغرات في خادم SSH المدمج قد تتيح لمهاجم الوصول إلى خدمات وملفات على خوادم أخرى يفترض أن يصل إليها المستخدم root فقط.

- أصدرت Tailscale الإصدار 1.104.4 لمعالجة ثغرات في خادم SSH المدمج فيها.
- قد تتيح الثغرات لمهاجم الوصول إلى خدمات وملفات على خوادم أخرى لا يفترض أن يصل إليها سوى root.
- تتعلق الثغرات بطريقة تمرير اتصالات الشبكة عبر Tailscale SSH.
- تنفذ عملية Tailscale الخلفية هذا التمرير بصلاحيات root.
- المقتطف المتاح من المصدر مبتور، لذا لم تتأكد شروط تنفيذ الهجوم.

أصدرت Tailscale الإصدار 1.104.4 لمعالجة ثغرات في خادم SSH المدمج فيها. وبحسب التقرير، قد تتيح هذه الثغرات لمهاجم الوصول إلى خدمات وملفات على خوادم أخرى لا يفترض أن يصل إليها سوى المستخدم root.

ما الذي يتأثر

تكمن المشكلة في طريقة تمرير Tailscale SSH لاتصالات الشبكة. وتتولى هذه المهمة عملية Tailscale الخلفية التي تعمل بصلاحيات root، ولهذا تكتسب أي ثغرة في هذا المسار أهمية، إذ يجري التمرير بصلاحيات أعلى بكثير من صلاحيات المستخدم العادي.

النص المتاح لدينا من المصدر مبتور عند الموضع الذي يشرح ما يلزم المهاجم لاستغلال الثغرات. لذلك لا يمكننا تحديد الشروط المسبقة بدقة، كما لا يرد في المقتطف أي أرقام CVE أو درجات خطورة. وننصح بالرجوع إلى ملاحظات الإصدار لدى الشركة لمعرفة التفاصيل.

الخطوات التالية

على الجهات التي تستخدم Tailscale SSH تحديد أماكن تشغيله وترقية تلك العقد إلى الإصدار 1.104.4. وإذا كانت الميزة تُستخدم للوصول إلى خوادم حساسة، فمن المفيد مراجعة الأجهزة المسموح لها بالاتصال بكل مضيف، لأن الخطر المذكور يتعلق بجهاز مخترق يصل إلى خوادم أخرى.

هذه مهمة ترقيع اعتيادية وليست حالة طارئة، لكن ينبغي تنفيذها وفق إدارة التغيير المعتمدة ومتابعتها حتى الإغلاق.

ما يجب فعله الآن

1. حصر جميع الخوادم والأجهزة التي تشغّل Tailscale SSH.
2. ترقية تثبيتات Tailscale المتأثرة إلى الإصدار 1.104.4 عبر إجراءات إدارة التغيير.
3. مراجعة ملاحظات الإصدار لدى الشركة لمعرفة شروط الاستغلال وأي توجيهات إضافية.
4. مراجعة قواعد الوصول التي تحدد الأجهزة المسموح لها بالاتصال بكل خادم عبر Tailscale SSH.
5. التأكد بعد الترقيع من أن العقد تعرض الإصدار المحدّث.