ثغرة حرجة بدرجة CVSS 10.0 في MicroCloudd LXD تتيح انتحال هوية عميل موثوق دون مفتاح خاص



ثغرة حرجة في MicroCloudd LXD من Canonical تتيح للمهاجم الدخول بصفة عميل موثوق باستخدام شهادته العامة فقط ووصول شبكي إلى واجهة HTTPS، مع إمكانية الوصول إلى العنقود والأجهزة الافتراضية.

- تؤثر الثغرة في MicroCloudd LXD من Canonical وتحمل تقييم CVSS 10.0.
- يمكن للمهاجم تسجيل الدخول بصفة عميل موثوق دون امتلاك مفتاحه الخاص.
- يتطلب الاستغلال الوصول الشبكي إلى واجهة HTTPS API والحصول على الشهادة العامة للعميل الموثوق.
- عند النجاح يتصرف المهاجم بصلاحيات ذلك العميل، مع وصول إلى العنقود والأجهزة الافتراضية.

ما الذي تم الإبلاغ عنه

كُشفت ثغرة حرجة في LXD وMicroCloudg من Canonical، وقد صُنّفت بدرجة CVSS 10.0 وهي الدرجة القصوى. وتتيح الثغرة للمهاجم المصادقة بصفة عميل موثوق دون امتلاك المفتاح الخاص لذلك العميل.

شروط الاستغلال

يحتاج المهاجم إلى أمرين: وصول شبكي إلى واجهة HTTPS API في البيئة المتأثرة، والحصول على الشهادة العامة للعميل الموثوق المراد انتحاله. والشهادة العامة لا تُعامل عادةً كسر، ولهذا تكتسب مسألة عدم الحاجة إلى المفتاح الخاص أهمية كبيرة. وبعد المصادقة يتصرف المهاجم بصفة ذلك العميل ويصل إلى العنقود والأجهزة الافتراضية. والنص المتاح من المصدر مقتطع عند الحديث عن الأثر إذا كان الحساب المنتحَل ذا صلاحيات أعلى، لذلك لا تتوفر هنا تفاصيل العواقب الكاملة.

لماذا يهم ذلك

ينبغي للجهات التي تستخدم LXD أو MicroCloud في السحابة الخاصة أو المحاكاة الافتراضية التعامل مع هذه الثغرة كأولوية، خصوصاً إذا كانت واجهة API قابلة للوصول من خارج شبكة إدارة مضبوطة بإحكام. ولا يذكر المصدر إصدارات التصحيح أو رقم CVE أو حالة الاستغلال، لذا يُرجع إلى إشعار Canonical الرسمي لهذه التفاصيل.

إلى حين تأكيد التصحيحات وتطبيقها، فإن تقليص الجهات القادرة على الوصول إلى الواجهة هو أنسب وسيلة عملية لخفض المخاطر.

ما يجب فعله الآن

1. حصر جميع نشرات LXD وMicroCloudg، بما فيها العناقيد في بيئات الاختبار والتطوير.
2. تقييد الوصول الشبكي إلى واجهة HTTPS API بشبكات الإدارة المخصصة والمضيفات المعتمدة فقط.
3. مراجعة إشعار Canonical الرسمي وتطبيق الإصدارات المصححة فور التأكد منها.
4. مراجعة سجلات الوصول إلى API والعنقود بحثاً عن نشاط عملاء غير متوقع أو مصادر غير مألوفة.
5. مراجعة شهادات العملاء الموثوقين المسجلة وإزالة غير المستخدم أو غير اللازم منها.