# เอกสารแจ้งเตือนกรณีพบช่องโหว่ใน AnyDesk เสี่ยงถูกยกระดับสิทธิ์เป็นผู้ดูแลระบบ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีพบช่องโหว่ใน AnyDesk เสี่ยงถูกยกระดับสิทธิ์เป็นผู้ดูแลระบบ

นักวิจัยด้านความปลอดภัยเปิดเผยช่องโหว่ในซอฟต์แวร์ AnyDesk ซึ่งเป็นเครื่องมือสำหรับเข้าถึงและจัดการคอมพิวเตอร์ระยะไกลที่ได้รับความนิยมทั่วโลก ที่ช่องโหว่ CVE-2024-12754 (มีคะแนน CVSS 5.5) และอาจถูกใช้เพื่อแพร่กระจายมัลแวร์หรือโจมตีโดยไม่ได้รับอนุญาต ช่องโหว่ดังกล่าวเกิดจากการที่ AnyDesk ทำงานภายใต้บัญชี NT AUTHORITY\SYSTEM ซึ่งมีสิทธิ์ระดับสูงสุดของระบบ ส่งผลให้สามารถคัดลอกไฟล์สำคัญ เช่น SAM, SYSTEM และ SECURITY ไปยัง C:\Windows\Temp ได้ แม้ว่าไฟล์เหล่านี้ยังคงรักษาสิทธิ์ระดับ SYSTEM แต่ผู้ใช้ที่มีสิทธิ์ต่ำสามารถเข้าถึงได้ ซึ่งอาจนำไปสู่การขโมยข้อมูลผู้ใช้หรือควบคุมระบบโดยไม่ได้รับอนุญาต

เพื่อป้องกันความเสี่ยง AnyDesk ได้ออกแพตช์แก้ไขในเวอร์ชัน 9.0.1 และแนะนำให้ผู้ใช้ทำการอัปเดตซอฟต์แวร์ทันที เพื่อป้องกันการโจมตีที่อาจเกิดขึ้น นอกจากนี้นักวิจัยยังระบุว่าผู้ใช้ที่มีสิทธิ์ต่ำสามารถตั้งค่าภาพพื้นหลังของตนเองได้ ซึ่งอาจถูกใช้ร่วมกับกลไกของระบบเพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต [1]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

**อ้างอิง**

1. https://securityonline.info/anydesk-exploit-alert-cve-2024-12754-enables-privilege-escalation-poc-available/?fbclid=IwZXh0bgNhZW0CMTEAAR0kW_0fjRQnTb2-ZPQGjJFFIS-Juy0_x9HaxvL2LEcvzw1iT3BdJ_ny8jY_aem_aBylbJYQgNCVkyz2Tt3MUA