วันที่ 5 กุมภาพันธ์ 2567

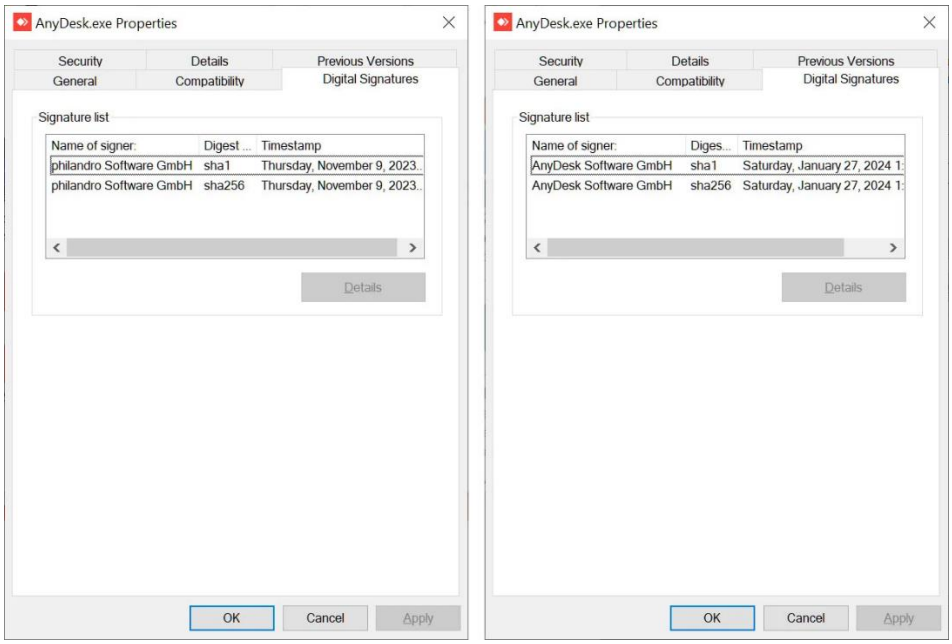
AnyDesk says hackers breached its production servers reset passwords

Executive Summary

ทางศูนย์ CSOC พบรายงานการแจ้งเตือนเกี่ยวกับการโจมตี AnyDesk ที่ถูกยืนยันว่าถูกโจมตีจริงที่อนุญาตให้แฮกเกอร์เข้าถึงระบบการผลิตของษริษัทได้ซึ่ง AnyDesk เป็นโซลูชันที่เกี่ยวกับการเข้าถึงระยะไกลที่อนุญาตให้ผู้ใช้เข้าถึงคอมพิวเตอร์ได้จากระยะไกลผ่านเครือข่ายซึ่งได้รับความนิยมอย่างมากจากองค์กร ซอฟต์แวร์นี้ยังได้รับความนิยมในกลุ่มแฮกเกอร์ที่ใช้ในการเข้าถึงอุปกรณ์และเครือข่าย

AnyDesk hacked

คำแถลงในบ่ายวันศุกร์ AnyDesk ได้รายงานว่าพวกเขาทราบถึงการโจมตีหลังจากตรวจพบสัญญาณของเหตุการณ์บนเซิร์ฟเวอร์การผลิตของพวกเขา หลังจากได้ทำการตรวจสอบความปลอดภัย พวกเขากำหนดว่าระบบได้รับการบุกรุกและได้เตรียมแผนการตอบสนองต่อเหตุการณ์พร้อมกับความได้รับความช่วยเหลือจากบริษัทรักษาความปลอดภัยด้านไอทีอย่าง CrowdStrike แต่ AnyDesk ยังไม่ได้รายงานเกี่ยวกับรายละเอียดการถูกโจมตีหรือข้อมูลที่ถูกขโมยในระหว่างการโจมตี อย่างไรก็ตามทำให้รู้ว่าผู้ที่ดำเนินการโจมตีได้ขโมยโค้ดต้นฉบับและใบรับรองการเขียนโค้ด (code signing certificates) ซึ่งทางบริษัทยังได้ยืนยันว่าไม่มี Ransomware มาเกี่ยวข้องแต่ก็ไม่ได้แชร์ข้อมูลมากเกี่ยวกับการโจมตีนี้ นอกจากการระบุว่าเซิร์ฟเวอร์ของพวกเขาถูกโจมตี โดยมีคำแนะนำน้อยมากเกี่ยวกับวิธีที่พวกเขาตอบสนองต่อเหตุการณ์ แม้ว่าบริษัทจะระบุว่าไม่มีการขโมย Authentication tokens แต่เพื่อความมั่นใจ AnyDesk ได้แนะนำให้เปลี่ยนรหัสผ่านและกล่าวว่า AnyDesk ได้รับการออกแบบในลักษณะที่ไม่สามารถขโมยโทเค็นที่มีอยู่ในอุปกรณ์ของผู้ใช้งานได้



Signed AnyDesk 8.0.6 (left) vs AnyDesk 8.0.8 (right) Source: BleepingComputer

ประกาศที่ AnyDesk ได้ยืนยันว่าการดูแลรักษารักษาความปลอดภัยที่เกิดขึ้นกับ my.anydesk II ซึ่งในการปฏิบัติการดูแลรักษารักษาความปลอดภัยนี้ได้รับการเชื่อมโยงกับเหตุการณ์ทางไซเบอร์ที่มีส่งผลกระทบกับ AnyDesk โดยที่ Günter Born ได้รายงานว่า AnyDesk ประสบปัญหาที่ยาวนานและบริษัทได้ปิดการใช้งานความสามารถในการเข้าสู่ AnyDesk client และข้อความในหน้าสถานะว่า my.anydesk II กำลังรับการบำรุงรักษาที่คาดว่าจะสามารถใช้งานได้อย่างปกติภายใน 48 ชั่วโมงหรือน้อยกว่านั้น การเข้าถึงถูกเปิดใช้งานใหม่เมื่อวานนี้ทำให้ผู้ใช้สามารถเข้าสู่ระบบได้ แต่ AnyDesk ไม่ได้ให้ข้อมูลเพิ่มเติมเกี่ยวกับเหตุผลของการดูแลรักษาในการอัพเดตสถานะ AnyDesk และขอนำให้ผู้ใช้งานไปใช้เวอร์ชันใหม่ของซอฟต์แวร์ เนื่องจากใบรับรองการเขียนโค้ดเก่าจะถูกเพิกถอนในเร็วๆนี้ นอกจากนี้ถึงแม้ AnyDesk จะรายงานว่ารหัสผ่านไม่ได้ถูกขโมยในการโจมตี แต่ผู้ให้บริการยืนยันว่าผู้โจมตีได้เข้าถึงระบบการผลิตดังนั้นขอแนะนำให้ผู้ใช้ AnyDesk ทุกคนเปลี่ยนรหัสผ่านของตนเอง

ศูนย์ CSOC แนะนำให้ลูกค้าตรวจสอบรายละเอียดด้านความปลอดภัยของระบบที่ใช้งานภายในองค์กรรวมการตรวจสอบและประเมินความปลอดภัยของระบบสารสนเทศและเครือข่าย โดยมุ่งเน้นที่ปัญหาในด้านความปลอดภัยของระบบและเพื่อลดความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้ช่องโหว่นี้เป็นช่องโหว่ที่ก่อให้เกิดความเสี่ยงที่ยอมรับไม่ได้ต่อองค์กรควรต้องมีการดำเนินการตรวจสอบเพื่อลดความเสี่ยง ทั้งนี้ในช่วงเวลาที่รายงานฉบับนี้ออก (2 ก.พ. 2567) และยังพบ Proof-of-concept code สำหรับการโจมตีช่องโหว่นี้และยังพบรายงานเกี่ยวกับการโจมตีช่องโหว่เหล่านี้ในอินเทอร์เน็ต

รายละเอียดของช่องโหว่โดยสรุป

- ผลิตภัณฑ์ที่ได้รับผลกระทบ: AnyDesk
- หน่วยงานที่ออกคำแนะนำด้านความปลอดภัย: AnyDesk
- ผลกระทบ (Impact): AnyDesk reset passwords
- การแก้ไขปัญหา:
    - หากเป็นผู้ใช้ AnyDesk ควรเปลี่ยนรหัสผ่านของคุณทันทีและหากใช้รหัสผ่านเดียวกันในเว็บไซต์อื่นๆ ควรเปลี่ยนรหัสผ่านในนั้นเช่นกัน
    - การอัพเดตซอฟต์แวร์ AnyDesk ให้เป็นเวอร์ชันล่าสุด
    - ควรตรวจสอบหน้าสถานะหรือแจ้งเตือนจากระบบที่ AnyDesk ได้ให้มา

ข้อมูลที่พบจาก Threat intelligence

- ในช่วงเวลาที่รายงานฉบับนี้ออก (2 ก.พ. 2567) ยังพบ Proof-of-concept code สำหรับการโจมตีช่องโหว่นี้ และยังพบรายงานเกี่ยวกับการโจมตีช่องโหว่เหล่านี้ในอินเทอร์เน็ต

ทั้งนี้การแก้ไข Configuration เพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว ลูกค้าควรปฏิบัติตาม Change Management Policy หรือ Risk Management Policy หรือ Business Impact Assessment ของหน่วยงานอย่างเคร่งครัด

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/