วันที่ 10 สิงหาคม 2569

มัลแวร์สามารถใช้คีย์ Windows Hello for Business เพื่อรักษาการเข้าถึง Entra ID ได้อย่างต่อเนื่อง

นักวิจัยด้าน Entra ID Dirk-jan Mollema แสดงให้เห็นว่า มัลแวร์ที่กำลังทำงานอยู่ใน Session ของ Windows ที่ผู้ใช้ลงชื่อเข้าใช้แล้ว สามารถใช้คีย์ Windows Hello for Business ของผู้ใช้โดยที่ผู้ใช้ไม่รู้ตัว เพื่อยืนยันตัวตนเข้าสู่ Microsoft Entra ID ได้ จากนั้นผู้โจมตีสามารถสร้างช่องทางการเข้าถึง Cloud ที่อยู่ได้นานขึ้น ลงทะเบียนอุปกรณ์ที่ผู้โจมตีควบคุม ขอรับ Primary Refresh Token (PRT) และเพิ่มวิธีการยืนยันตัวตนเพิ่มเติมได้ หากนโยบายของ Tenant อนุญาต

ในระบบที่ใช้ TPM เพื่อปกป้องคีย์ ผู้โจมตีไม่จำเป็นต้องดึง Private Key ออกมา ไม่จำเป็นต้องกู้ PIN และไม่จำเป็นต้องทำให้ระบบแสดงหน้าต่างขอการยืนยันด้วย Biometrics ระบบ Ticketing ของ Windows ยังคงเปิดให้สามารถใช้งานกระบวนการที่เกี่ยวข้องกับ Private Key ได้ในขณะที่ผู้ใช้กำลังลงชื่อเข้าใช้และใช้งานเครื่องอยู่ ทำให้โค้ดที่ทำงานภายใต้สิทธิ์ของผู้ใช้สามารถขอให้ Windows สร้างข้อมูลสำหรับการยืนยันตัวตนได้ โดยไม่จำเป็นต้องมีสิทธิ์ระดับ Administrator

เทคนิคนี้จำเป็นต้องมีโค้ดที่สามารถทำงานได้ภายใน Session ที่ผู้เสียหายลงชื่อเข้าใช้อยู่ Mollema อธิบายว่าพฤติกรรมดังกล่าวเป็นผลจากวิธีการทำงานของ Windows Hello for Business และระบุว่าพฤติกรรมนี้ยังคงถูกปล่อยไว้ตามเดิม การเปิดเผยข้อมูลครั้งนี้ไม่ได้รายงานว่ามีการนำเทคนิคดังกล่าวไปใช้โจมตีจริง หรือมีผู้เสียหายแล้ว โดย Mollema แนะนำให้ตรวจสอบการลงทะเบียนอุปกรณ์ที่ไม่คาดคิด

ข้อมูลที่เปิดเผยไม่ได้ระบุ Windows Build ที่แน่นอน หรือรูปแบบการติดตั้ง Windows Hello for Business ที่ใช้ในการทดสอบ The Hacker News ไม่พบหมายเลข CVE หรือคำแนะนำด้านความปลอดภัยจาก Microsoft ที่เชื่อมโยงกับเทคนิคนี้จากการค้นหาใน Microsoft Security Update Guide, NVD และ CVE.org ณ วันที่ 6 สิงหาคม 2026 โดย The Hacker News ได้ติดต่อ Microsoft และ Mollema แล้ว และอยู่ระหว่างรอคำตอบ

Microsoft มีเอกสารอธิบายพฤติกรรมของระบบ Ticketing ดังกล่าว ส่วน Mollema ระบุว่า ความสามารถในการเรียกใช้คีย์ Windows Hello for Business จาก Session ที่ถูกบุกรุก เคยถูกนำเสนอในงาน DEF CON 32 เมื่อปี 2024 วิธีดังกล่าวสามารถสร้าง Signed Assertion สำหรับ PRT ได้ แต่ยังจำเป็นต้องเข้าถึงอุปกรณ์ที่ลงทะเบียนหรือเข้าร่วมกับ Entra อยู่ก่อน

งานวิจัยครั้งใหม่นี้ตัดข้อกำหนดดังกล่าวออก โดยนำคีย์ Windows Hello for Business มาใช้งานในลักษณะ FIDO2 Passkey ผ่าน WebAuthn Mollema พบว่า Challenge ของ Entra ID ซึ่งมีอายุ 5 นาที ไม่ได้ผูกไว้กับ Session, ผู้ใช้ หรือ Tenant ใดโดยเฉพาะ

ดังนั้น ผู้โจมตีสามารถขอ Challenge จาก Host เครื่องอื่น และสั่งให้ Endpoint ที่ถูกบุกรุกสร้าง Signed Assertion ให้ได้ จากนั้น ROADtools ซึ่งเป็น Framework สำหรับโต้ตอบกับ Entra ID สามารถนำ Assertion ดังกล่าวไปขอ Token หรือเปิด Browser Session ในฐานะผู้เสียหายได้

Mollema พบว่า Token ดังกล่าวไม่มี Device ID Claim การไม่มีการผูก Token เข้ากับอุปกรณ์เปิดโอกาสให้ผู้โจมตีลงทะเบียนอุปกรณ์ใหม่ ขอ PRT สำหรับอุปกรณ์ดังกล่าว และเข้าถึงบริการ Cloud ของ Microsoft ได้ โดย Microsoft ระบุว่า PRT มีอายุ 90 วัน และจะได้รับการต่ออายุอย่างต่อเนื่องในขณะที่ผู้ใช้ยังใช้งานอุปกรณ์อย่างต่อเนื่อง

Mollema พบว่าการลงชื่อเข้าใช้ผ่าน WebAuthn สามารถตอบสนองข้อกำหนดของ Conditional Access ที่บังคับใช้ระดับการยืนยันตัวตนแบบป้องกันการ Phishing ของ Microsoft ได้ นอกจากนี้เขาระบุว่าการลงชื่อเข้าใช้ดังกล่าวยังถูกนับเป็นการยืนยันตัวตนแบบ Multi-Factor Authentication ที่เพิ่งเกิดขึ้น ทำให้ผู้โจมตีสามารถเพิ่ม Passkey หรือคีย์ Windows Hello for Business ลงในอุปกรณ์ใหม่ได้ หากนโยบายอนุญาต อย่างไรก็ตาม นโยบายแยกต่างหากที่ตรวจสอบสถานะของอุปกรณ์หรือการปฏิบัติตามข้อกำหนดอาจสามารถหยุดการโจมตีไว้ได้ ดังนั้นเส้นทางการรักษาการเข้าถึงแบบถาวรนี้จึงไม่สามารถทำงานได้กับทุกสภาพแวดล้อม

การค้นพบนี้แสดงให้เห็นข้อจำกัดอย่างหนึ่งของการยืนยันตัวตนที่ป้องกันการ Phishing แม้ Credential จะยังคงถูกผูกไว้กับ Hardware และไม่สามารถส่งออกได้ แต่มัลแวร์ที่อยู่ภายใน Session ของ Endpoint ที่ผู้ใช้ลงชื่อเข้าใช้อยู่ก็ยังสามารถเรียกใช้ Credential ดังกล่าวเพื่อประโยชน์ของผู้โจมตีได้

Mollema เผยแพร่ Script สำหรับทำ Proof-of-Concept ที่เขียนด้วย PowerShell ไว้ใน Repository ของ ROADtools โดย The Hacker News พบไฟล์ fido_assertion.ps1 และ hellopoc.ps1 อยู่ในโฟลเดอร์ดังกล่าวเมื่อวันที่ 6 สิงหาคม 2026 สำหรับการตรวจจับ Mollema แนะนำให้ค้นหาการลงชื่อเข้าใช้ด้วย Windows Hello for Business ที่มี Device ID เป็นค่าว่าง อย่างไรก็ตาม Session ของ Browser แบบ Incognito หรือ Session ที่ไม่ได้ใช้ SSO อย่างถูกต้องก็สามารถทำให้เกิดรูปแบบเดียวกันได้

ข้อมูลอ้างอิง

Aug 07, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/08/malware-can-abuse-windows-hello-for.html