แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนกรณีผู้ไม่หวังดีเข้ายึดบัญชี Microsoft 365 ผ่านหน้าจอลงทะเบียน Microsoft Entra Passkey ปลอม

วันที่แจ้งเตือน 20 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่ข่าวการโจมตีรูปแบบใหม่จากกลุ่มผู้ไม่หวังดีที่มุ่งเป้าขโมยบัญชีผู้ใช้งาน Microsoft 365 โดยหลอกลวงให้ผู้ใช้งานดำเนินการลงทะเบียน Passkey โดยมีรายละเอียดดังนี้

การโจมตี

ผู้ไม่หวังดีใช้ Phishing Kit ผ่านแผงควบคุม (PHP Panel) และสามารถตอบสนองต่อระบบของเหยื่อได้แบบเรียลไทม์ โดยมีขั้นตอนดังนี้

1. การดักจับข้อมูลการเข้าสู่ระบบ (Credential Phishing)
   - เหยื่อถูกนำไปยังเว็บไซต์ปลอมที่เลียนแบบ Microsoft Entra Passkey และให้กรอก Username และ Password โดยข้อมูลดังกล่าวจะถูกส่งไปยังผู้ไม่หวังดีทันที
2. การหลอกให้ยืนยัน MFA
   - เว็บไซต์ปลอมจะแสดงหน้าจอตามขั้นตอน MFA ที่ระบบจริงร้องขอ
   - เหยื่อกรอก OTP หรือกดยืนยัน MFA โดยไม่รู้ว่าถูกหลอก
3. การลงทะเบียน Passkey
   - หลังจากเหยื่อยืนยัน MFA สำเร็จ จะถูกเปลี่ยนเส้นทางไปยังหน้าตั้งค่า Passkey หรือหน้ากู้คืนคีย์เพื่อเบี่ยงเบนความสนใจ
   - ผู้ไม่หวังดีทำการเพิ่ม Passkey ของตนเองเข้ากับบัญชีเหยื่อ
4. การยึดครองบัญชี Microsoft 365
   - ผู้โจมตีใช้ Passkey ที่ผูกไว้เข้าสู่ระบบเพื่อเข้าถึงอีเมล ไฟล์ และบริการต่างๆ ของ Microsoft 365 และนำไปใช้เรียกค่าไถ่ได้

เว็บปลอม ⟶ ขโมย Username/Password ⟶ หลอกให้ยืนยัน MFA ⟶ แอบเพิ่ม Passkey ของแฮกเกอร์ ⟶ ยึดบัญชี Microsoft 365

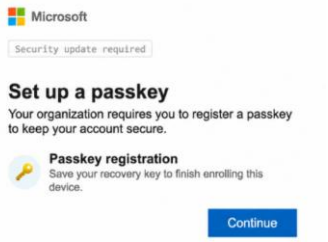
ผลกระทบ

กลุ่มอุปกรณ์ที่เข้าข่ายได้รับผลกระทบ

- บัญชีผู้ใช้งานระบบ Microsoft 365 และระบบการจัดการข้อมูลประจำตัว Microsoft Entra ID

รูปแบบการแพร่กระจายและการโจมตี

- การหลอกลวงผ่านเสียง (Vishing) ผู้โจมตีจะโทรศัพท์หาเหยื่อโดยตรงเพื่อโน้มน้าวหรือสร้างความตื่นตระหนก ว่าบัญชีมีความเสี่ยง และจำเป็นต้องลงทะเบียน Passkey ใหม่
- ใช้ชื่อโดเมนที่จดทะเบียนใหม่โดยมีคำว่า "passkey" เพื่อสร้างความน่าเชื่อถือให้กับลิงก์ฟิชชิง
- การฉวยโอกาสจากความไม่คุ้นเคย จากการที่หลายองค์กรกำลังผลักดันการใช้ Passkey ตามนโยบายของ Microsoft และอาศัยความไม่คุ้นเคยของผู้ใช้กับหน้าจอการตั้งค่า Passkey ของจริง



แนวทางการป้องกันและลดความเสี่ยง

- บังคับใช้ระบบยืนยันตัวตนที่ป้องกันการหลอกลวงได้ (Phishing-resistant MFA) เช่น พาสคีย์ (Passkeys) หรือสมาร์ทการ์ด เป็นต้น เพื่อทดแทนการใช้รหัสผ่านผ่าน SMS หรือ TOTP ซึ่งจะช่วยบล็อกการเข้าสู่ระบบของผู้โจมตีได้โดยตรง
- กำหนดและปฏิบัติตามขั้นตอนการยืนยันตัวตนของเจ้าหน้าที่ฝ่ายสนับสนุน (Support) ทุกครั้งที่มีการโทรติดต่อผู้ใช้งานเพื่อป้องกันการสวมรอย
- ปิดกั้นคำขอเข้าถึงระบบจากพื้นที่หรือประเทศที่องค์กรไม่ได้ดำเนินธุรกิจอยู่ (ผ่านการกรองประเทศ, ASN หรือ IP)
- จำกัดการเข้าถึงแอปพลิเคชันที่สำคัญ ให้ใช้งานได้เฉพาะบนอุปกรณ์ขององค์กร ที่ติดตั้งระบบรักษาความปลอดภัยแล้วเท่านั้น
- แจ้งเตือนผู้ใช้งานทุกครั้งที่มีการเปลี่ยนแปลงวิธีการยืนยันตัวตน รวมถึงเมื่อมีการเพิ่มพาสคีย์ (Passkey) ใหม่เข้าสู่ระบบบัญชี

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 18 ก.ค. 2569
2. https://thehackernews.com/2026/07/hackers-use-fake-microsoft-entra.html?
3. https://www.okta.com/en-au/blog/threat-intelligence/vishing-actors-target-microsoft-entra-passkey-enrollment-/?

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Windows File System Proxy (WinFsp) ออก Security Patch แก้ไขช่องโหว่ในผลิตภัณฑ์ (CVE-2026-7162)

วันที่แจ้งเตือน 20 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่ข่าวเกี่ยวกับช่องโหว่ใน Windows File System Proxy หรือ WinFsp โดยมีรายละเอียดดังนี้

รายละเอียดช่องโหว่	ผลกระทบ
• Windows File System Proxy หรือ WinFsp เป็นซอฟต์แวร์โอเพนซอร์สที่ช่วยให้นักพัฒนาสามารถสร้างและเชื่อมต่อระบบไฟล์เสมือนบนระบบปฏิบัติการ Windows โดย WinFsp ไม่ใช่ส่วนประกอบมาตรฐานที่ติดตั้งมาพร้อมกับ Windows แต่อาจถูกติดตั้งโดยตรงหรือใช้เป็นส่วนประกอบในซอฟต์แวร์อื่น • CVE-2026-7162 เป็นช่องโหว่ประเภท Integer Overflow ใน WinFsp ที่อาจทำให้เกิดความผิดพลาดในการจัดการข้อมูลภายในระบบ	• ผู้ไม่หวังดีที่สามารถเข้าถึงระบบที่ได้รับผลกระทบอาจใช้ประโยชน์จากช่องโหว่เพื่อยกระดับสิทธิและดำเนินการบนระบบด้วยสิทธิระดับ SYSTEM ส่งผลให้ผู้โจมตีอาจเรียกใช้คำสั่ง เข้าถึง หรือแก้ไขข้อมูล ติดตั้งโปรแกรม หรือเปลี่ยนแปลงการตั้งค่าที่สำคัญของระบบได้ • กระทบต่อ WinFsp เวอร์ชัน 2.2.26112 และ เวอร์ชันก่อนหน้า
แนวทางการแก้ไข: • อัปเดตเป็น WinFsp 2026 Beta 2 (v2.2B2) เวอร์ชัน 2.2.26183 • ตรวจสอบว่าเครื่องแม่ข่าย เครื่องผู้ใช้งาน หรือระบบจัดเก็บข้อมูลภายในองค์กรมีการติดตั้ง WinFsp หรือไม่ • ตรวจสอบซอฟต์แวร์อื่นที่อาจติดตั้งหรือใช้งาน WinFsp เป็นส่วนประกอบ แม้ผู้ดูแลระบบไม่ได้ติดตั้ง WinFsp โดยตรง • จำกัดการใช้งานบัญชีผู้ดูแลระบบเฉพาะกรณีที่จำเป็น และหลีกเลี่ยงการใช้งานบัญชีสิทธิสูงในการปฏิบัติงานทั่วไป	**มาตรการชั่วคราวหากยังไม่สามารถอัปเดตได้ทันที:** • จำกัดการเข้าถึงระบบที่มีการติดตั้ง WinFsp เฉพาะผู้ใช้งานและผู้ดูแลระบบที่จำเป็น • ปิดใช้งานหรือนำซอฟต์แวร์ที่ใช้งาน WinFsp ออกจากระบบชั่วคราว หากไม่กระทบต่อการให้บริการ • จำกัดสิทธิการเข้าสู่ระบบแบบ Local และ Remote ของบัญชีผู้ใช้งานที่ไม่จำเป็น • ตรวจสอบบัญชีผู้ใช้งานที่มีสิทธิเข้าถึงเครื่องหรือระบบที่ได้รับผลกระทบ • เปิดใช้งานมาตรการป้องกันของระบบปฏิบัติการ เช่น EDR และ Application Control เป็นต้น

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 18 ก.ค. 2569
2. https://nvd.nist.gov/vuln/detail/CVE-2026-7162?
3. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-086/