วันที่ 28 มกราคม 2569

Microsoft Office Zero-Day (CVE-2026-21509) – ออกแพตช์ฉุกเฉิน หลังพบการโจมตีจริง

เมื่อวันจันทร์ที่ผ่านมา Microsoft ได้ออกแพตช์ความปลอดภัยแบบเร่งด่วน (Out-of-band) เพื่อแก้ไขช่องโหว่ Zero-Day ระดับความรุนแรงสูงใน Microsoft Office ซึ่งถูกนำไปใช้โจมตีจริงแล้ว ช่องโหว่นี้ถูกติดตามภายใต้รหัส CVE-2026-21509 และมีคะแนนความรุนแรง (CVSS) อยู่ที่ 7.8 จาก 10 โดย Microsoft อธิบายว่าเป็นช่องโหว่ประเภทการข้ามกลไกความปลอดภัย (Security Feature Bypass) ใน Microsoft Office

รายละเอียดเชิงเทคนิคของช่องโหว่

Microsoft ระบุในคำแนะนำด้านความปลอดภัยว่า “การพึ่งพาข้อมูลที่ไม่น่าเชื่อถือในการตัดสินใจด้านความปลอดภัยใน Microsoft Office อาจทำให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถข้ามกลไกป้องกันบางอย่างได้จากเครื่องของผู้ใช้โดยตรง การอัปเดตนี้ช่วยแก้ไขช่องโหว่ที่สามารถข้ามระบบป้องกัน OLE ใน Microsoft 365 และ Microsoft Office ซึ่งมีหน้าที่ป้องกันผู้ใช้จาก COM/OLE control ที่มีความเสี่ยง”

ลักษณะการโจมตี: การโจมตีจะเกิดขึ้นได้เมื่อผู้โจมตีส่งไฟล์ Office ที่ถูกสร้างขึ้นมาเป็นพิเศษ และหลอกให้เหยื่อเปิดไฟล์นั้นขึ้นมา อย่างไรก็ตาม Microsoft ยืนยันว่า Preview Pane ไม่ใช่ช่องทางในการโจมตี

เวอร์ชันที่ได้รับผลกระทบและการป้องกัน

1. Microsoft 365 และ Office 2021 หรือใหม่กว่า: ผู้ใช้กลุ่มนี้จะได้รับการป้องกันโดยอัตโนมัติผ่านการปรับตั้งค่าฝั่งเซิร์ฟเวอร์ แต่มีเงื่อนไขสำคัญคือ จำเป็นต้องปิดและเปิดโปรแกรม Office ใหม่ เพื่อให้การป้องกันมีผล

2. Microsoft Office 2016 และ 2019: จำเป็นต้องติดตั้งอัปเดตตามรายการเลขเวอร์ชันต่อไปนี้:

- **Microsoft Office 2019 (32-bit edition):** 16.0.10417.20095
- **Microsoft Office 2019 (64-bit edition):** 16.0.10417.20095
- **Microsoft Office 2016 (32-bit edition):** 16.0.5539.1001

- **Microsoft Office 2016 (64-bit edition):** 16.0.5539.1001

วิธีป้องกันชั่วคราว (Workaround) โดยการแก้ไข Registry

ในระหว่างนี้ Microsoft แนะนำให้ใช้วิธีป้องกันชั่วคราวผ่านการแก้ไขค่าใน Windows Registry ตามขั้นตอนอย่างละเอียดดังนี้:

ข้อควรระวัง: โปรดสำรองข้อมูล Registry ก่อนดำเนินการ, ปิดโปรแกรม Microsoft Office ทุกตัว และเปิด Registry Editor ขึ้นมา

ไปยังตำแหน่ง Registry ที่ตรงกับการติดตั้ง Office ของคุณ:

- **สำหรับ Office แบบ MSI 64-bit หรือ Office 32-bit บน Windows 32-bit:**
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Common\COM Compatibility\
- **สำหรับ Office แบบ MSI 32-bit บน Windows 64-bit:**
  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\
- **สำหรับ Office แบบ Click-to-Run 64-bit หรือ Office 32-bit บน Windows 32-bit:**
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\Microsoft\Office\16.0\Common\COM Compatibility\
- **สำหรับ Office แบบ Click-to-Run 32-bit บน Windows 64-bit:**
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\REGISTRY\MACHINE\Software\WOW6432Node\Microsoft\Office\16.0\Common\COM Compatibility\

ขั้นตอนการสร้าง Key และ Value:

1. คลิกขวาที่โฟลเดอร์ COM Compatibility แล้วเลือก Add Key
2. ตั้งชื่อ Key ใหม่เป็น: {EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}
3. คลิกขวาที่ Key ที่สร้างใหม่ เลือก New > DWORD (32-bit) Value
4. ตั้งชื่อค่าเป็น "Compatibility Flags" และกำหนดค่าแบบ Hexadecimal เป็น 400
5. ปิด Registry Editor และเปิดโปรแกรม Office ขึ้นมาใหม่

ข้อมูลเพิ่มเติมและการตอบสนองจากหน่วยงานรัฐ

Microsoft ยังไม่ได้เปิดเผยรายละเอียดเกี่ยวกับรูปแบบหรือขอบเขตของการโจมตีที่ใช้ช่องโหว่นี้ โดยได้ให้เครดิตแก่ทีมงานผู้ค้นพบดังนี้:

- Microsoft Threat Intelligence Center (MSTIC)
- Microsoft Security Response Center (MSRC)
- Office Product Group Security Team

จากเหตุการณ์ดังกล่าว หน่วยงานด้านความมั่นคงไซเบอร์ของสหรัฐฯ หรือ CISA ได้เพิ่มช่องโหว่นี้เข้าไปในรายการ Known Exploited Vulnerabilities (KEV) และกำหนดให้หน่วยงานภาครัฐของสหรัฐฯ (FCEB) ต้องดำเนินการแก้ไขให้แล้วเสร็จภายในวันที่ 16 กุมภาพันธ์ 2026

ข้อมูลอ้างอิง

Jan 27, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/microsoft-issues-emergency-patch-for.html