แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณีการโจมตี Microsoft 365 ด้วย FastHTTP และ Microsoft พบช่องโหว่แบบ Zero-day จำนวน 8 รายการ

วันที่แจ้งเตือน 16 มกราคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ พบว่า บริษัท SpearTip ผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เผยแพร่กรณีพบการโจมตีทางไซเบอร์รูปแบบใหม่ที่มุ่งเป้าไปที่บัญชีผู้ใช้บน Microsoft 365 โดยการทำ Brute-force Attack ผ่าน FastHTTP Library ซึ่งผู้โจมตีใช้เพื่อส่งคำร้องขอเข้าสู่ระบบจำนวนมากไปยัง Azure Active Directory Graph API โดยมีการใช้รายการรหัสผ่านที่รั่วไหลจากเหตุการณ์ข้อมูลรั่วไหลในอดีต รวมทั้งยังพบการโจมตีด้วยวิธี MFA Fatigue ซึ่งเป็นการส่งคำร้องขอยืนยันตัวตนแบบหลายปัจจัย (MFA) ซ้ำ ๆ ไปยังอุปกรณ์ เพื่อก่อกวนและหลอกเหยื่อให้ยินยอมเข้าถึงบัญชีผู้ใช้

การโจมตีนี้มีอัตราความสำเร็จสูงถึง 9.7% ซึ่งถือว่าสูงกว่าปกติมาก โดยอาจก่อให้เกิดความเสียหาย เช่น การขโมยข้อมูลที่เป็นความลับ การเข้าถึงทรัพย์สินทางปัญญา การแพร่กระจายการโจมตีไปยังระบบอื่นภายในองค์กร และการหยุดชะงักของบริการ เป็นต้น

นอกจากนี้ ไมโครซอฟท์ ได้เปิดเผยช่องโหว่ด้านความปลอดภัยที่สำคัญจำนวน 159 รายการในการอัปเดตประจำเดือนมกราคม 2568 โดยพบว่ามีช่องโหว่ที่ยังไม่ได้รับการแก้ไข (Zero-day) ถึง 8 รายการ ซึ่งมีความเสี่ยงสูงเป็นพิเศษ โดยเฉพาะช่องโหว่ในระบบ Windows Hyper-V (รหัส CVE-2025-21333 CVE-2025-21334 และ CVE-2025-21335) ที่กำลังถูกใช้โจมตีเพื่อยกระดับสิทธิเป็นระดับ SYSTEM รวมทั้งยังพบช่องโหว่ในระบบติดตั้งแพ็กเกจของ Windows (CVE-2025-21275) ที่อาจถูกใช้ในการยกระดับสิทธิ และช่องโหว่ในส่วน Windows Themes (CVE-2025-21308) ที่อาจทำให้ข้อมูลยืนยันตัวตน NTLM รั่วไหล เมื่อมีการแสดงไฟล์ธีมที่ถูกดัดแปลงพิเศษ

ช่องโหว่ดังกล่าวเปิดโอกาสให้ผู้ไม่ประสงค์ดีสามารถโจมตีระบบได้หลายรูปแบบ โดยเฉพาะการยกระดับสิทธิ โดยไม่ได้รับอนุญาตผ่านช่องโหว่ใน Windows Hyper-V ซึ่งอาจนำไปสู่การเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต นอกจากนี้ยังพบความเสี่ยงจากการโจมตีผ่านช่องโหว่ใน Microsoft Office และ SharePoint รวมถึงการส่งอีเมลที่แนบไฟล์อันตราย และการหลบเลี่ยงระบบรักษาความปลอดภัยผ่านช่องโหว่ใน Windows SmartScreen ได้

CVE ID	CVE Title
CVE-2025-21333 CVE-2025-21334 CVE-2025-21335	Windows Hyper-V NTKernel Integration VSPElevation of PrivilegeVulnerability
CVE-2025-21308	Windows ThemesSpoofing Vulnerability
CVE-2025-21275	Windows App PackageInstaller Elevation ofPrivilege Vulnerability

แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง องค์กรควรดำเนินมาตรการป้องกันและรับมืออย่างรอบด้าน เริ่มจากการปรับปรุงระบบความปลอดภัยทางเทคนิค โดยเฉพาะในระบบ Microsoft 365 ด้วยการเพิ่มความเข้มงวดในการยืนยันตัวตนแบบหลายปัจจัย เพิ่มการควบคุมการอนุญาตเข้าถึงจาก Trusted Location และการติดตั้งระบบป้องกันการโจมตีแบบ Brute Force พร้อมทั้งอัปเดตระบบความปลอดภัยให้เป็นปัจจุบันอยู่เสมอ ควบคู่ไปกับการเฝ้าระวังและตรวจสอบระบบอย่างต่อเนื่อง โดยเฉพาะการตรวจสอบบันทึกการเข้าถึงระบบ การตรวจหาการใช้งาน FastHTTP และพฤติกรรมผิดปกติต่าง ๆ รวมทั้งควรให้ความสำคัญกับการบริหารจัดการผู้ใช้งาน ทั้งการกำหนดนโยบายรหัสผ่าน การจัดการสิทธิ และการให้ความรู้แก่พนักงานเกี่ยวกับภัยคุกคามรูปแบบใหม่ ๆ รวมถึงการจัดทำระบบสำรองข้อมูลที่มีประสิทธิภาพและแผนความต่อเนื่องทางธุรกิจ พร้อมกำหนดช่องทางการสื่อสารและประสานงานที่ชัดเจนระหว่างทีมด้านความมั่นคงปลอดภัย ผู้บริหาร และหน่วยงานภายนอก ทั้งนี้ การติดตามข่าวสารและการแจ้งเตือนภัยคุกคามอย่างสม่ำเสมอจะช่วยให้องค์กรสามารถปรับตัวและรับมือกับภัยคุกคามที่เปลี่ยนแปลงได้อย่างทันท่วงที

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/hackers-use-fasthttp-in-new-high-speed-microsoft-365-password-attacks/
2. https://windowsforum.com/threads/hackers-exploit-fasthttp-for-brute-force-attacks-on-microsoft-365.349438/
3. https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2025-patch-tuesday-fixes-8-zero-days-159-flaws/
4. https://socradar.io/january-2025-patch-tuesday-8-zero-days-159-cves/