แจ้งเตือน

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

แจ้งเตือนช่องโหว่ Zero Day ของผลิตภัณฑ์ Microsoft จำนวน 3 รายการ (CVE-2025-62221, CVE-2025-64671 และ CVE-2025-54100)

วันที่แจ้งเตือน 18 ธันวาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่าบริษัท Microsoft ได้ออก Security Patch ประจำเดือนธันวาคม 2568 เพื่อแก้ไขช่องโหว่สำคัญ จำนวน 57 รายการ รวมถึงช่องโหว่ระดับร้ายแรง Zero-Days จำนวน 3 รายการ ได้แก่

1. **CVE-2025-62221** เป็นช่องโหว่ Elevation of Privilege ใน Windows Cloud Files Mini Filter Driver ที่ผู้ไม่ประสงค์ดีได้นำไปใช้โจมตีแล้ว ช่องโหว่นี้เกิดจากปัญหา use-after-free ในไดรเวอร์ ทำให้ผู้โจมตีที่มีสิทธิ์เข้าถึงระบบและสามารถยกระดับสิทธิ์ (Privilege Escalation) เป็น System ซึ่งเป็นสิทธิ์สูงทำให้ควบคุมระบบขององค์กรได้ ทั้งนี้ Microsoft ยังไม่ได้เปิดเผยรายละเอียดเชิงเทคนิคเกี่ยวกับวิธีการโจมตีที่ถูกนำมาใช้ดังกล่าว

2. **CVE-2025-64671** เป็นช่องโหว่ Remote Code Execution ใน GitHub Copilot for JetBrains ซึ่งผู้ไม่ประสงค์ดีสามารถสั่งรันคำสั่งในเครื่องของผู้ใช้งานได้ ช่องโหว่นี้เกิดจากการจัดการคำสั่งที่ไม่เหมาะสม (Command Injection) ทำให้ช่องโหว่นี้ถูกใช้ผ่านเทคนิค Cross Prompt Injection เข้าโจมตี

3. **CVE-2025-54100** เป็นช่องโหว่ Remote Code Execution ใน Windows PowerShell ทำให้สคริปต์ที่ฝังอยู่ในหน้าเว็บถูกเรียกใช้งานโดยอัตโนมัติ เมื่อผู้ใช้ดึงข้อมูลหน้าเว็บดังกล่าวผ่านคำสั่ง Invoke-WebRequest

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ผู้ประกอบธุรกิจควรพิจารณาดำเนินการติดตั้ง Patch ตามคำแนะนำของผู้ออกผลิตภัณฑ์ ตรวจสอบและเฝ้าระวังกิจกรรมที่ผิดปกติในระบบ โดยเฉพาะการพยายามยกระดับสิทธิ์หรือการเข้าถึงระบบที่ไม่ได้รับอนุญาต สำรองข้อมูลสำคัญอย่างสม่ำเสมอ และทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติ เพื่อให้สามารถจัดการแก้ไขเหตุการณ์ได้ตามที่กำหนด

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2025-patch-tuesday-fixes-3-zero-days-57-flaws/
2. https://www.cve.org/CVERecord?id=CVE-2025-62221
3. https://www.cve.org/CVERecord?id=CVE-2025-64671
4. https://www.cve.org/CVERecord?id=CVE-2025-54100