แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ Zero Day ของผลิตภัณฑ์ Microsoft จำนวน 2 รายการ (CVE-2025-55234 และ CVE-2024-21907)

วันที่แจ้งเตือน 17 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงาน ก.ล.ต. ร่วมกับ TCM-CERT ได้ติดตามข่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์พบรายงาน Patch Tuesday ประจำเดือนกันยายน 2568 ของผลิตภัณฑ์ Microsoft สำหรับแก้ไขช่องโหว่ จำนวน 81 รายการ โดยมี (1) ช่องโหว่ที่ส่งผลกระทบร้ายแรง (Critical) จำนวน 9 รายการ และ (2) ช่องโหว่ประเภท Zero Day จำนวน 2 รายการ (CVE-2025-55234 และ CVE-2024-21907) โดยพบว่าช่องโหว่ Zero Day ดังกล่าว ได้เปิดเผยสู่สารธารณะหรือใช้ประโยชน์แล้ว ซึ่งเป็นช่องโหว่ของผลิตภัณฑ์ Windows SMB Server และ Microsoft SQL Server Microsoft ตามลำดับ โดยมีรายละเอียดดังนี้

ZeroDay CVE ID	ผลิตภัณฑ์ที่ได้รับผลกระทบ	รายละเอียดช่องโหว่	ผลกระทบ
CVE-2025-55234	Windows 10,11 และ Windows Server ตามที่ระบุในอ้างอิง 2	ช่องโหว่ Windows SMB Elevation of Privilege Vulnerability	SMB Server อาจมีความเสี่ยงต่อการถูกโจมตีแบบรีเลย์ (relay attacks) ขึ้นอยู่กับการกำหนดค่า และผู้ไม่หวังดีทำการยกระดับสิทธิ (elevation of privilege) ของตนเองในระบบได้
วิธีป้องกันหรือแก้ไข: Microsoft ได้ออกคำแนะนำให้ผู้ใช้งานดำเนินการดังต่อไปนี้ เพื่อป้องกันตนเองจากการโจมตี • ประเมินสภาพแวดล้อม โดยใช้ความสามารถในการตรวจสอบ (audit capabilities) ที่มีให้ในชุดอัปเดตความปลอดภัยประจำเดือนกันยายน 2025 โดยศึกษาเอกสาร Support for Audit Events to deploy SMB Server Hardening (อ้างอิง 3) • นำมาตรการเสริมความมั่นคงปลอดภัยของ SMB Server มาใช้ อย่างเหมาะสม			
CVE-2024-21907	Newtonsoft.Json เวอร์ชันก่อนหน้า 13.0.1	ช่องโหว่ Improper Handling of Exceptional Conditions การจัดการข้อผิดพลาดที่ไม่ถูกต้องใน Newtonsoft.Json	ผู้โจมตีที่ไม่ได้ยืนยันตัวตน (unauthenticated remote attacker) อาจส่งข้อมูลที่ถูกสร้างขึ้น (crafted data) ไปยัง method “JsonConvert.DeserializeObject” ทำให้เกิด Stack Overflow และส่งผลให้เกิด Denial of Service (DoS) ได้
วิธีป้องกันหรือแก้ไข: Microsoft ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดต SQL Server เวอร์ชันที่เกี่ยวข้อง ตามที่แนะนำโดยเร็วที่สุด (อ้างอิง 4)			

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

ข้อมูลอ้างอิง

1) https://www.bleepingcomputer.com/news/microsoft/microsoft-september-2025-patch-tuesday-fixes-81-flaws-two-zero-days/?
2) https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-55234
3) https://support.microsoft.com/en-us/topic/support-for-audit-events-to-deploy-smb-server-hardening-smb-server-signing-smb-server-epa-056f7478-ee2c-43b9-b94b-c0ff06de1d8f
4) https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21907