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

แจ้งเตือน Microsoft ออก Security Patch ช่องโหว่ระดับร้ายแรง (CVE-2025-55241) ใน Microsoft Entra ID

วันที่แจ้งเตือน 23 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ และพบว่าบริษัท Microsoft ได้ออกและติดตั้ง Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรง (CVE-2025-55241) ใน Microsoft Entra ID (เดิมชื่อ Azure AD) ซึ่งเกิดจากความบกพร่องในการตรวจสอบ actor token ที่ใช้ในการเชื่อมต่อแบบ service-to-service (S2S) ที่ไม่รัดกุมเพียงพอส่งผลให้ผู้ไม่ประสงค์ดีสามารถนำ token จาก tenant ไปใช้ใน tenant อื่นได้ โดยยกระดับสิทธิ์ขึ้นเป็นผู้ดูแลระบบสูงสุด (Global Admin Privilege Escalation) ได้ ซึ่งทำให้สามารถเข้าถึงและควบคุมระบบและข้อมูลซึ่งส่งผลกระทบต่อความลับ ความถูกต้อง และความพร้อมใช้ของระบบ และอาจทำให้องค์กรอาจไม่สามารถตรวจจับการโจมตีได้ทันท่วงที

มาตรการป้องกันและแนวทางปฏิบัติ เพื่อป้องกันภัยคุกคามจากช่องโหว่นี้ สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบ พิจารณาดำเนินมาตรการที่เหมาะสมเพื่อรับมือกับช่องโหว่ Microsoft Entra ID ตรวจสอบให้มั่นใจว่า tenant ของหน่วยงานได้ถูกติดตั้ง Security Patch ล่าสุดโดย Microsoft แล้ว ตรวจสอบสิทธิ์ Global Admin ภายในระบบอย่างสม่ำเสมอ เพิ่มการเฝ้าระวังการเข้าถึงหรือพฤติกรรมที่ผิดปกติของผู้ใช้งาน ทั้งนี้ การดำเนินมาตรการเชิงรุกดังกล่าวจะช่วยลดความเสี่ยงและเสริมความมั่นคงปลอดภัยให้แก่หน่วยงานได้

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

ข้อมูลอ้างอิง

1. https://arstechnica.com/security/2025/09/microsofts-entra-id-vulnerabilities-could-have-been-catastrophic/
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55241
3. https://thehackernews.com/2025/09/microsoft-patches-critical-entra-id.html