

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณี ตรวจพบช่องโหว่ระดับรุนแรงใน Windows Server 2025 เสี่ยงต่อการยกระดับสิทธิ์ใน Active Directory

วันที่แจ้งเตือน 26 พฤษภาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบการธุรกิจหลักทรัพย์และผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารภัยคุกคามทางไซเบอร์และพบกรณีรายงานเกี่ยวกับช่องโหว่ของพีเจอร์ Delegated Managed Service Account (dMSA) ในระบบ Windows Server 2025 เพิ่มเข้ามาเพื่อเสริมความปลอดภัยของการตรวจสอบสิทธิ์ในระบบ Kerberos โดยผู้ไม่ประสงค์ดีอาจใช้ช่องโหว่ดังกล่าว ยกระดับสิทธิ์เพื่อควบคุม Active Directory ได้อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบและข้อมูล การปฏิบัติงาน และความต่อเนื่องทางธุรกิจโดยรวมได้

เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น สำนักงาน ก.ล.ต. ขอแจ้งเตือนให้บริษัทและหน่วยงานท่าน พิจารณาดำเนินการที่เหมาะสมเพื่อติดตาม ทบทวนและจำกัดสิทธิ์ของผู้ใช้ กรณีที่มีการใช้งาน dMSA ทั้งนี้ นักวิจัยของ Akamai ได้ให้คำแนะนำในการ Mitigate Risk โดยเผยแพร่สคริปต์ PowerShell ที่อาจใช้เพื่อช่วยผู้ดูแลระบบ ตรวจสอบบัญชีผู้ใช้ที่มีสิทธิ์เกี่ยวข้องกับ dMSA และเฝ้าระวังภัยคุกคามจากช่องโหว่นี้อย่างใกล้ชิด

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบการในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบการทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

- <https://thehackernews.com/2025/05/critical-windows-server-2025-dmsa.html>
- <https://windowsforum.com/threads/critical-analysis-of-windows-server-2025-dmsa-privilege-escalation-vulnerability.367584/>
- <https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory#badsuccessor>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ