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

แจ้งเตือนช่องโหว่ร้ายแรงของผลิตภัณฑ์ MS Exchange Server (CVE-2024-21410)

วันที่แจ้งเตือน 16 กุมภาพันธ์ 2567

ไมโครซอฟท์ได้แจ้งเตือนช่องโหว่ร้ายแรง (CVE-2024-21410) ของผลิตภัณฑ์ MS Exchange Server ซึ่งส่งผลให้ผู้ไม่หวังดีอาศัยช่องโหว่นี้เพื่อยกระดับสิทธิ (Escalate Privilege) บน MS Exchange Server ด้วยการโจมตีผ่าน New Technology LAN Manager (NTLM) Relay ซึ่งเป็นรูปแบบการโจมตีในลักษณะ man-in-the-middle (MITM) โดยอาศัยการขโมยข้อมูลยืนยันตัวตน (credentials) จากเครื่องเป้าหมาย (NTLM client เช่น โปรแกรม MS Outlook เป็นต้น) ระหว่างที่ทำการเชื่อมต่อกับเครื่องแม่ข่ายปลายทาง (NTLM server เช่น MS Exchange Server เป็นต้น)

ทั้งนี้ ซอฟต์แวร์เวอร์ชันที่ได้รับผลกระทบ ได้แก่

- Microsoft Exchange Server 2016 Cumulative Update 23
- Microsoft Exchange Server 2019 Cumulative Update 13 ตั้งแต่เวอร์ชัน 15.02.0 ไปจนถึงก่อนเวอร์ชัน 15.2.1544.004
- Microsoft Exchange Server 2019 Cumulative Update 14 ตั้งแต่เวอร์ชัน 15.02.0 ไปจนถึงก่อนเวอร์ชัน 15.2.1544.004

ไมโครซอฟท์ได้ออกคำแนะนำเพื่อป้องกันผลกระทบจากช่องโหว่ ดังนี้

- MS Exchange Server 2019 : ติดตั้ง Cumulative Update 14 ซึ่งจะเปิดใช้งานฟีเจอร์ NTLM credentials MS Exchange Relay Protections โดยอัตโนมัติ (หากไม่สามารถเปิดใช้งานฟีเจอร์ดังกล่าวได้ให้ทำตามคำแนะนำเพิ่มเติมในข้อมูลอ้างอิง 1)
- MS Exchange Server 2016 : จะไม่ได้รับ Cumulative Update แต่ยังมีวิธีป้องกันช่องโหว่โดยการเปิดใช้งานฟีเจอร์ Extended Protection (คำแนะนำเพิ่มเติมใน FAQ ของข้อมูลอ้างอิง 2)

ผู้ประกอบธุรกิจควรพิจารณาติดตั้งโปรแกรมแก้ไขช่องโหว่ (Patch) และตั้งค่าระบบตามที่ไมโครซอฟต์แนะนำ โดยควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง พร้อมทั้งจัดให้มีมาตรการควบคุมอย่างเหมาะสม เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นจากการติดตั้ง Patch หรือเปลี่ยนแปลงการตั้งค่าระบบ

ข้อมูลอ้างอิง

1) https://techcommunity.microsoft.com/t5/exchange-team-blog/released-2024-h1-cumulative-update-for-exchange-server/ba-p/4047506
2) https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21410
3) https://support.microsoft.com/en-au/topic/cumulative-update-14-for-exchange-server-2019-kb5035606-5d08ad6d-3527-41c9-82b6-e19d3ddf94db
4) https://www.bleepingcomputer.com/news/security/microsoft-new-critical-exchange-bug-exploited-as-zero-day/