แจ้งเตือน : ช่องโหว่	ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : White
HIGH	☒ Financial Damage ☒ Reputation Damage ☐ Non-compliance ☒ Privacy Violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ Zero-day บน Microsoft Exchange Server (CVE-2022-41040) และ (CVE-2022-41082)

วันที่แจ้งเตือน 1 ตุลาคม 2565

เมื่อ วันที่ 29 กันยายน 2565 Microsoft แจ้งเตือนช่องโหว่แบบ zero day ที่ตรวจพบบนโปรแกรม Microsoft Exchange Server แบบ on-premises (ไม่ส่งผลกระทบกับ Microsoft Exchange Online) โดยพบช่องโหว่ 2 รายการ ได้แก่ CVE-2022-41040 ซึ่งเป็นช่องโหว่ประเภท Server-Side Request Forgery (SSRF) และ CVE-2022-41082 ซึ่งเป็นช่องโหว่ประเภท Remote Code Execution (RCE) ที่ใช้คำสั่งจากระยะไกลผ่านทางโปรแกรม PowerShell ได้ ผู้ไม่หวังดีจึงสามารถอาศัยช่องโหว่ดังกล่าวในการติดตั้งโปรแกรมต่าง ๆ เพื่อเรียกดู เปลี่ยนแปลงหรือลบข้อมูล หรือสร้างบัญชีผู้ใช้งานใหม่พร้อมสิทธิผู้ใช้งานในระดับผู้ดูแลระบบ (administrative rights) หรือ สิทธิผู้ใช้งานระดับสูง (privilege account) บนระบบที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบ

ทั้งนี้ ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Microsoft Exchange Server เวอร์ชัน 2013, 2016 และ 2019 ซึ่งปัจจุบัน Microsoft ยังไม่ได้ออกชุดอัปเดตเพื่อแก้ไขช่องโหว่ (Security Patch) อย่างไรก็ดี เบื้องต้น Microsoft ได้ออกคำแนะนำในการบรรเทาผลกระทบและการตรวจจับ เพื่อช่วยให้ผู้ใช้งานสามารถป้องกันตนเองจากการโจมตีเหล่านี้ได้ โดยแนะนำให้เพิ่มกฎเพื่อปิดกั้นคำร้องขอจากผู้ไม่หวังดี (Request with indicators of attack) ผ่านโมดูล URL Rewrite Rule บนเซิร์ฟเวอร์ Internet Information Services (IIS) และปิดกั้นพอร์ตที่ใช้สำหรับ Remote PowerShell (HTTP: 5985 และ HTTPS: 5986) **โดยเร็วที่สุด**จนกว่า Microsoft จะออกชุดอัปเดตเพื่อแก้ไขช่องโหว่ (สามารถดูรายละเอียดเพิ่มเติมจากเอกสารอ้างอิง)

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น บริษัทควรแนะนำให้บุคลากรภายในองค์กรดำเนินการตามที่ Microsoft แนะนำ โดยผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนดำเนินการ

ข้อมูลอ้างอิง

1) https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
2) https://www.csa.gov.sg/singcert/Alerts/al-2022-056
3) https://drive.google.com/file/d/16U1b1lldKURf5AEJWzHcYEIU60rx8N8E/view