แจ้งเตือน : ช่องโหว่

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 แก้ไขช่องโหว่ระดับร้ายแรง (CVE-2025-49719) ในผลิตภัณฑ์ Microsoft Window Server

วันที่แจ้งเตือน 27 ตุลาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารเกี่ยวกับการโจมตีทางไซเบอร์ และพบว่า Microsoft ได้ออก Security Patch ช่องโหว่ระดับร้ายแรง (CVE-2025-59287) ในผลิตภัณฑ์ Windows Server Update Services (WSUS)

ช่องโหว่นี้เปิดโอกาสให้ผู้ไม่ประสงค์ดีสามารถส่งคำสั่งโจมตีจากระยะไกลได้ (Remote Code Execution - RCE) บนเซิร์ฟเวอร์ WSUS ได้โดยไม่ต้องมีบัญชีผู้ใช้หรือการพิสูจน์ตัวตน (unauthenticated) เมื่อโจมตีโดยใช้สิทธิ์ของระบบ (SYSTEM Privileges) เพื่อสั่ง malware ให้ทำงานแล้ว อาจสามารถควบคุมการทำงานและก่อความเสียหายร้ายแรงต่อระบบและเครือข่ายภายในองค์กรได้

เพื่อป้องกันและลดความเสี่ยงดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการติดตั้ง Security Patch ตามที่ Microsoft แจ้ง (Out-of-Band Security Update) เพื่อแก้ไขช่องโหว่ดังกล่าวบนเซิร์ฟเวอร์ WSUS และตรวจสอบให้มั่นใจว่าเซิร์ฟเวอร์ WSUS นั้น อนุญาตให้เข้าถึงได้เฉพาะจากเครื่องหรือผู้ใช้ที่อยู่ในเครือข่ายที่จำเป็นเท่านั้น เพื่อลดความเสี่ยงที่จะเกิดขึ้นได้

เวอร์ชั่นผลิตภัณฑ์	รหัส Patch
Windows Server 2025	KB5070881
Windows Server, version 23H2	KB5070879
Windows Server 2022	KB5070884
Windows Server 2019	KB5070883
Windows Server 2016	KB5070882
Windows Server 2012 R2	KB5070886
Windows Server 2012	KB5070887

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/microsoft-releases-windows-server-emergency-updates-for-critical-wsus-rce-flaw/
2. https://www.bleepingcomputer.com/news/security/hackers-now-exploiting-critical-windows-server-wsus-flaw-in-attacks/
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59287