วันที่ 5 พฤศจิกายน 2568

CISA และ NSA ออกคำแนะนำเร่งด่วนเพื่อรักษาความปลอดภัยของ WSUS และ Microsoft Exchange Server

หน่วยงานความมั่นคงทางไซเบอร์ของสหรัฐฯ (CISA) และสำนักงานความมั่นคงแห่งชาติ (NSA) ร่วมกับพันธมิตรจากออสเตรเลียและแคนาดา ได้ออกคำแนะนำด้านความปลอดภัยชุดใหม่ที่ถือเป็นเรื่องเร่งด่วน เพื่อให้องค์กรต่าง ๆ เสริมความปลอดภัยให้กับระบบ Microsoft Exchange Server แบบติดตั้งภายในองค์กร (on-premise) และเตือนภัยช่องโหว่ Windows Server Update Services (WSUS) ที่ถูกโจมตีจริงในโลกไซเบอร์

1. คำแนะนำเพื่อเสริมเกราะ Exchange Server (Zero Trust)

หน่วยงานต่าง ๆ ย้ำว่าการโจมตีระบบ Microsoft Exchange Server ยังคงดำเนินอยู่อย่างต่อเนื่อง โดยเฉพาะระบบที่ขาดการป้องกันหรือตั้งค่าผิดพลาด องค์กรต่าง ๆ ควรยกเลิกการใช้งาน Exchange Server รุ่นเก่าที่หมดอายุ และย้ายไปใช้ Microsoft 365 แทน CISA ระบุว่า การนำแนวคิดการรักษาความปลอดภัยแบบ Zero Trust มาใช้ ซึ่งถือเป็นสิ่งสำคัญอย่างยิ่ง

“ด้วยการจำกัดสิทธิ์การเข้าถึงของผู้ดูแลระบบ เปิดใช้งานการยืนยันตัวตนหลายขั้นตอน (Multi-factor Authentication) กำหนดค่าความปลอดภัยของระบบรับส่งข้อมูลให้เข้มงวด และนำแนวคิดการรักษาความปลอดภัยแบบ Zero Trust มาใช้ องค์กรจะสามารถเสริมความแข็งแกร่งให้กับระบบป้องกันการโจมตีทางไซเบอร์ได้อย่างมาก”

แนวทางปฏิบัติที่แนะนำอย่างละเอียด:

การอัปเดตและการย้ายระบบ: ติดตั้งอัปเดตด้านความปลอดภัยและแพตช์อย่างสม่ำเสมอ ย้ายระบบ Exchange Server รุ่นเก่าที่หมดอายุการใช้งาน ออกจากระบบ และตรวจสอบให้แน่ใจว่าบริการ Exchange Emergency Mitigation ยังคงเปิดใช้งานอยู่

มาตรการป้องกัน Endpoint: ใช้และบำรุงรักษามาตรฐานความปลอดภัยของ Exchange Server, Windows และโปรแกรมรับส่งอีเมล โดยเปิดใช้งานโปรแกรมป้องกันไวรัส, ส่วนติดต่อ Windows Antimalware Scan Interface (AMSI), ฟีเจอร์ Attack Surface Reduction (ASR), AppLocker และ App Control for Business, ระบบตรวจจับและตอบสนอง (Endpoint Detection and Response), รวมถึงฟีเจอร์ป้องกันสแปมและมัลแวร์ของ Exchange Server

การจำกัดสิทธิ์ (Least Privilege): ใช้หลักการสิทธิ์ขั้นต่ำ (least privilege) โดยจำกัดสิทธิ์การเข้าถึงของผู้ดูแลระบบใน Exchange Admin Center (EAC) และ PowerShell ระยะไกล และปิดการเข้าถึง PowerShell ระยะไกล ของผู้ใช้ทั่วไปใน Exchange Management Shell (EMS)

การยืนยันตัวตนและการเข้ารหัส: เสริมความปลอดภัยในการยืนยันตัวตนและการเข้ารหัส โดยตั้งค่า Transport Layer Security (TLS), HTTP Strict Transport Security (HSTS), Extended Protection (EP), ใช้ Kerberos และ Server Message Block (SMB) แทน NTLM และเปิดใช้งาน multi-factor authentication

หน่วยงานระบุว่า: “การรักษาความปลอดภัยของ Exchange Server เป็นสิ่งสำคัญ เพื่อคงไว้ซึ่งความถูกต้องและความลับของการสื่อสารและการทำงานภายในองค์กร... การประเมินและเสริมความมั่นคงทางไซเบอร์ของเซิร์ฟเวอร์สื่อสารเหล่านี้อย่างต่อเนื่อง เป็นสิ่งจำเป็นในการป้องกันภัยคุกคามที่พัฒนาอย่างต่อเนื่อง”

2. คำเตือนภัย Zero-Day: ช่องโหว่ WSUS (CVE-2025-59287) ถูกโจมตีจริง

คำแนะนำด้านความปลอดภัยนี้ถูกเผยแพร่เพียงหนึ่งวันหลังจากที่ CISA ออกอัปเดตการแจ้งเตือนเกี่ยวกับช่องโหว่ CVE-2025-59287 ซึ่งเป็นช่องโหว่ด้านความปลอดภัยในส่วนประกอบ Windows Server Update Services (WSUS) ที่อาจทำให้เกิดการ รันโค้ดจากระยะไกล (Remote Code Execution) ได้

Sophos รายงานว่าผู้โจมตีกำลังใช้ช่องโหว่นี้เพื่อขโมยข้อมูลสำคัญจากองค์กรในสหรัฐฯหลายแห่ง ครอบคลุมตั้งแต่สถาบันการศึกษา, เทคโนโลยี, การผลิต, ไปจนถึงด้านสาธารณสุข โดยการโจมตีเริ่มตรวจพบครั้งแรกเมื่อวันที่ 24 ตุลาคม 2025 เพียงหนึ่งวันหลังจากที่ Microsoft ออกอัปเดตดังกล่าว

กลไกการโจมตีและสัญญาณเตือน

การโจมตีจริง: ผู้โจมตีใช้ประโยชน์จาก WSUS Server ที่มีช่องโหว่ เพื่อรันคำสั่ง PowerShell ที่เข้ารหัสด้วย Base64 และส่งผลลัพธ์ออกไปยังปลายทาง webhook[.]site ซึ่งสอดคล้องกับรายงานจาก Darktrace, Huntress และ Unit 42 ของ Palo Alto Networks

สถิติการถูกโจมตี: บริษัท Sophos เปิดเผยกับ The Hacker News ว่าพบเหตุการณ์ดังกล่าวแล้ว 6 กรณี ในระบบของลูกค้า และยังพบว่ามีเหยื่ออย่างน้อย 50 ราย ตามการวิจัยเพิ่มเติม

คำเตือนล่วงหน้า: Rafe Pilling จาก Sophos Counter Threat Unit กล่าวว่า "เหตุการณ์นี้แสดงให้เห็นว่าผู้โจมตีสามารถปรับตัวและลงมือโจมตีช่องโหว่สำคัญใน WSUS ได้อย่างรวดเร็ว... เป็นไปได้ว่านี่อาจเป็นการทดสอบหรือขั้นตอนการสำรวจข้อมูลในเบื้องต้น... เรายังไม่พบการโจมตีในวงกว้างในตอนนี้ แต่ถือว่านี่เป็นสัญญาณเตือนล่วงหน้า องค์กรควรรีบติดตั้งแพตช์ล่าสุดและกำหนดค่า WSUS ให้ปลอดภัย เพื่อลดความเสี่ยงจากการถูกโจมตี”

การตรวจสอบและติดตั้งแพตช์เร่งด่วน:

CISA แนะนำให้องค์กรต่าง ๆ ตรวจสอบว่าเซิร์ฟเวอร์ใดบ้างที่อาจถูกโจมตีได้ และติดตั้ง แพตช์นอกกำหนด (out-of-band update) ที่ Microsoft ปล่อยออกมา

สัญญาณกิจกรรมที่น่าสงสัยที่ต้องเฝ้าระวัง:

- เฝ้าดูกิจกรรมหรือกระบวนการลูก (child processes) ที่ถูกสร้างขึ้นด้วยสิทธิ์ SYSTEM โดยเฉพาะอย่างยิ่งที่มาจากไฟล์ wsusservice.exe และ/หรือ w3wp.exe
- เฝ้าระวังคำสั่ง PowerShell ที่ซ้อนกันหลายชั้น (nested) ซึ่งมีการเข้ารหัสด้วย Base64

เส้นทางการโจมตีที่ซับซ้อน (Splunk)

Michael Haag วิศวกรวิจัยภัยคุกคามอาวุโสจาก Splunk ระบุผ่านโพสต์ใน X ว่า ช่องโหว่ CVE-2025-59287 “มีความซับซ้อนกว่าที่คาดไว้” และพบเส้นทางการโจมตีอีกแบบหนึ่งที่ใช้โปรแกรม Microsoft Management Console (“mmc.exe”) เพื่อเรียกใช้ “cmd.exe” เมื่อผู้ดูแลเปิด WSUS Admin Console หรือคลิก “Reset Server Node”

ผลกระทบทางเทคนิค: “เส้นทางนี้ทำให้เกิดการ แครชของ Event Log รหัส 7053” Haag อธิบายเพิ่มเติม พร้อมระบุว่ามีรูปแบบการทำงานเหมือนกับที่บริษัท Huntress พบในไฟล์ “C:\Program Files\Update Services\Logfiles\SoftwareDistribution.log”

องค์กรต่าง ๆ ต้องเร่งติดตั้งแพตช์ล่าสุดและกำหนดค่า WSUS ให้ปลอดภัย เพื่อลดความเสี่ยงจากการถูกโจมตี เนื่องจากภัยคุกคามมีการพัฒนาอย่างต่อเนื่อง

เพื่อให้ง่ายต่อการตรวจสอบว่ารายละเอียดครบถ้วนหรือไม่ ผมสามารถจัดทำสรุปประเด็นหลักทั้งหมดที่คุณต้องการเน้นย้ำในแต่ละส่วนเป็นรายการตรวจสอบได้นะครับ

ข้อมูลอ้างอิง

Oct 31, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/cisa-and-nsa-issue-urgent-guidance-to.html