

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

ช่องโหว่ในผลิตภัณฑ์ Microsoft และ SonicWall เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 9 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Microsoft และ SonicWall เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	- ช่องโหว่ CVE-2026-96940 เป็นช่องโหว่ประเภท Privilege Escalation ใน Microsoft Exchange Server เกิดจากปัญหากระบวนการยืนยันตัวตนที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนสามารถยกระดับสิทธิผ่านเครือข่ายและเข้าถึง Mailbox ของผู้ใช้งานภายในองค์กร ทำให้เข้าถึงอีเมลและไฟล์แนบได้ - Microsoft แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าวแบบ On-Premises ดำเนินการอัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อ ผลิตภัณฑ์ - Microsoft Exchange Server Subscription Edition RTM เวอร์ชัน 15.02.0.0 ถึง เวอร์ชันก่อน 15.02.2562.053 - Microsoft Exchange Server 2016 Cumulative Update 23 เวอร์ชัน 15.01.0.0 ถึงเวอร์ชันก่อน 15.01.2507.075 - Microsoft Exchange Server 2019 Cumulative Update 15 เวอร์ชัน 15.02.0.0 ถึงเวอร์ชันก่อน 15.02.1748.053 - Microsoft Exchange Server 2019 Cumulative Update 14 เวอร์ชัน 15.02.0.0 ถึงเวอร์ชันก่อน 15.02.2562.053

ข้อมูลอ้างอิง Microsoft

- <https://nvd.nist.gov/vuln/detail/cve-2026-96940>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96940>
- <https://thehackernews.com/2026/10/microsoft-exchange-flaw-lets.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT
Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

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

ช่องโหว่ในผลิตภัณฑ์ Microsoft และ SonicWall เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 9 ตุลาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
SonicWall	- ช่องโหว่ CVE-2026-102255 เป็นช่องโหว่ประเภท Server-Side Request Forgery (SSRF) แบบ Pre-Authentication ใน WorkPlace Portal ของอุปกรณ์ SonicWall Secure Mobile Access (SMA) 1000 Gateway ซึ่งผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้เพื่อโจมตีจากระยะไกลโดยไม่ต้องผ่านการยืนยันตัวตน สามารถส่งคำสั่งที่สร้างขึ้นเพื่อเข้าถึงฟังก์ชันการทำงานภายในของอุปกรณ์และทำการโจมตีเพิ่มเติมได้ - แนะนำให้ผู้ใช้ผลิตภัณฑ์ SonicWall Secure Mobile Access (SMA) 1000 VPN ติดตั้ง Hotfix เวอร์ชันล่าสุด	ส่งผลกระทบต่อผลิตภัณฑ์ SMA 1000 Gateway รุ่น 6210, 7210 และ 8200v ที่ใช้ซอฟต์แวร์เวอร์ชัน 12.4.3-03526 หรือต่ำกว่า และ 12.5.0-02952 หรือต่ำกว่า

ข้อมูลอ้างอิง SonicWall

- <https://nvd.nist.gov/vuln/detail/cve-2026-102255>
- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017>
- <https://securityaffairs.com/200569/security/sonicwall-fixes-max-severity-pre-auth-flaw-in-sma1000-appliances.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ