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

Microsoft, SonicWall และ Zoom ออก Security Patch เพื่อแก้ไขช่องโหว่ที่ถูกใช้โจมตี

วันที่แจ้งเตือน 17 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft, SonicWall และ Zoom ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	• Cybersecurity and Infrastructure Security Agency (CISA) ได้ออกประกาศเตือนเกี่ยวกับช่องโหว่ใน Microsoft SharePoint Server (Self-hosted) ถูกนำไปใช้โจมตีจริง ได้แก่ CVE-2026-32201 (Improper Input Validation) CVE-2026-45659 (Deserialization of Untrusted Data) และ CVE-2026-56164 (Missing Authentication for Critical Function) โดยผู้ไม่หวังดีสามารถหลีกเลี่ยงการยืนยันตัวตน จากนั้นจะสั่งรันโค้ดอันตรายจากระยะไกลเพื่อดำเนินการโจมตีระบบได้ รวมทั้ง ขโมย Internet Information Services (IIS) และการเข้าถึงระบบอย่างต่อเนื่องเพื่อติดตั้งมัลแวร์บนระบบ • Microsoft แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อ Microsoft SharePoint Server เวอร์ชันที่ยังอยู่ในระยะการสนับสนุน รวมถึง SharePoint Server Subscription Edition เวอร์ชัน On-premises ที่ใช้รูปแบบการอัปเดตแบบต่อเนื่อง (Continuous Update)

ข้อมูลอ้างอิง Microsoft

1. https://nvd.nist.gov/vuln/detail/CVE-2026-32201
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201
3. https://nvd.nist.gov/vuln/detail/CVE-2026-45659
4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659
5. https://nvd.nist.gov/vuln/detail/CVE-2026-56164
6. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164
7. https://learn.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/security-hardening
8. https://www.bleepingcomputer.com/news/security/cisa-warns-admins-to-patch-actively-exploited-sharepoint-flaws/

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

Microsoft, SonicWall และ Zoom ออก Security Patch เพื่อแก้ไขช่องโหว่ที่ถูกใช้โจมตี

วันที่แจ้งเตือน 17 กรกฎาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
SonicWall	• ช่องโหว่ CVE-2026-15409 เป็นช่องโหว่ประเภท Server-Side Request Forgery (SSRF) ใน SonicWall ทำให้ผู้ไม่หวังดีสามารถโจมตีหรือสั่งรันโค้ดอันตรายได้จากระยะไกลโดยไม่ต้องยืนยันตัวตน จากนั้นสามารถควบคุมให้อุปกรณ์ส่งคำขอไปยังอุปกรณ์ปลายทางได้เพื่อโจมตี • ช่องโหว่ CVE-2026-15410 เป็นช่องโหว่ประเภท Code Injection หลังจากผู้ใช้งานยืนยันตัวตนแล้วในส่วน Appliance Management Console ของระบบ โดยผู้โจมตีที่ผ่านการยืนยันตัวตนและเข้าถึงระบบจากระยะไกลสามารถใช้ประโยชน์จากช่องโหว่นี้เพื่อสั่งรันคำสั่งบนระบบปฏิบัติการในสิทธิ์ระดับ administrator ได้ • SonicWall แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ SonicWall Secure Mobile Access (SMA) 1000 รุ่น 6210, 7210 และ 8200v
Zoom	• ช่องโหว่ CVE-2026-53412 เป็นช่องโหว่ประเภท Improper Input Validation ใน Zoom Workplace สำหรับ Windows ทำให้ผู้ไม่หวังดีสามารถเข้าควบคุมบัญชีผู้ใช้จากระยะไกลผ่านเครือข่ายได้ โดยไม่ต้องยืนยันตัวตน เมื่อโจมตีสำเร็จอาจจะสวมรอยเป็นเจ้าของบัญชี เข้าถึงระบบและโจมตีระบบเพิ่มเติมได้ • Zoom แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ • Zoom Workplace สำหรับ Windows เวอร์ชัน เก่ากว่า 7.0.5 • Zoom Workplace VDI Client for Windows เวอร์ชัน 7.0.5, 6.6.14 หรือ 6.5.17 • Zoom Meeting SDK for Windows เวอร์ชันก่อน 7.0.0

ข้อมูลอ้างอิง SonicWall

1. https://nvd.nist.gov/vuln/detail/CVE-2026-15409
2. https://nvd.nist.gov/vuln/detail/CVE-2026-15410
3. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
3. https://securityaffairs.com/195364/hacking/sonicwall-warns-of-active-exploitation-of-two-sma-1000-zero-days.html

ข้อมูลอ้างอิง Zoom

1. https://nvd.nist.gov/vuln/detail/CVE-2026-53412
2. https://www.zoom.com/en/trust/security-bulletin/zsb-26014/
3. https://thehackernews.com/2026/07/zoom-patches-critical-windows-flaw-that.html