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

Cisco และ SonicWall ออก Patch แก้ไขช่องโหว่ในผลิตภัณฑ์

วันที่แจ้งเตือน 22 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cisco และ SonicWall ได้ออก Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์ ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	• ช่องโหว่ CVE-2026-20223 เกิดจากกระบวนการตรวจสอบและยืนยันตัวตนที่ไม่เพียงพอเมื่อเข้าถึง REST API endpoint ทำให้ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้เข้าถึงจากระยะไกลโดยไม่ได้ผ่านการยืนยันตัวตน สามารถยกระดับสิทธิ์เป็น Site Admin ผ่าน API Request ที่ถูกสร้างขึ้น และสามารถเข้าถึงข้อมูลภายในระบบ รวมถึงดำเนินการเปลี่ยนแปลงค่าการตั้งค่าอุปกรณ์ปลายทางของเหยื่อได้ • Cisco ได้ออก Patch แก้ไขสำหรับเวอร์ชัน 3.10.8.3 และ 4.0.3.17 ตามรายละเอียดในข้อมูลอ้างอิง 1	ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Cisco Secure Workload ทั้งรูปแบบ SaaS Deployment และ On-Premises Cluster Software Deployment
SonicWall	• ช่องโหว่ CVE-2024-12802 เกิดจากอุปกรณ์ไม่ได้บังคับใช้ MFA อย่างเหมาะสม ทำให้ผู้ไม่หวังดีที่มี Credential สามารถเข้าสู่ระบบและใช้วิธี Brute-force เพื่อเดารหัสผ่าน VPN และหลีกเลี่ยงระบบ Multi-Factor Authentication (MFA) บนอุปกรณ์ SonicWall Gen6 SSL-VPN ก่อนนำเครื่องมือที่เกี่ยวข้องกับการโจมตีแบบ Ransomware เข้าไปติดตั้งภายในเครือข่ายขององค์กรเป้าหมาย • SonicWall ได้ออก Patch แก้ไขในหลายอุปกรณ์ รวมถึงคำแนะนำสำหรับการดำเนินการ โดยมีรายละเอียดในข้อมูลอ้างอิง 2	ส่งผลกระทบกับอุปกรณ์ SonicWall Gen6 NSv, Gen6 Firewalls, Gen7 Firewalls, Gen8 Firewalls และ SMA100 (รวมถึงกรณีที่อุปกรณ์ติดตั้ง Patch ไม่สมบูรณ์)

ข้อมูลอ้างอิง 1 : Cisco

1. https://nvd.nist.gov/vuln/detail/CVE-2026-20223
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy
3. https://securityaffairs.com/192473/security/cisco-fixed-maximum-severity-flaw-cve-2026-20223-in-secure-workload.html

ข้อมูลอ้างอิง 2 : SonicWall

1. https://nvd.nist.gov/vuln/detail/CVE-2024-12802
2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0001
3. https://www.bleepingcomputer.com/news/security/hackers-bypass-sonicwall-vpn-mfa-due-to-incomplete-patching

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ