แจ้งเตือน

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

SonicWall ออก Security Patch แก้ไขช่องโหว่จำนวน 3 รายการ (CVE-2026-0204, CVE-2026-0205 และ CVE-2026-0206)

วันที่แจ้งเตือน 5 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า SonicWall ออก Security Patch (Firmware) เพื่อแก้ไขช่องโหว่จำนวน 3 รายการ ในระบบปฏิบัติการ SonicOS ซึ่งส่งผลกระทบต่ออุปกรณ์ไฟร์วอลล์กลุ่ม Gen 6, Gen 7 และ Gen 8 มีรายละเอียดของช่องโหว่ ดังนี้

- CVE-2026-0204 เป็นประเภท improper access control เกิดจากการควบคุมการเข้าถึงที่ไม่เหมาะสม ทำให้ผู้ไม่หวังดีสามารถจัดการ interface บนอุปกรณ์ได้
- CVE-2026-0205 เป็นประเภท post-authentication path traversal ทำให้ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนสามารถเข้าถึงไฟล์และไดเร็กทอรีที่อยู่นอกเหนือขอบเขตที่กำหนด ส่งผลกระทบต่อข้อมูลภายในได้
- CVE-2026-0206 เป็นประเภท post-authentication stack-based buffer overflow ทำให้ผู้ไม่หวังดีส่งคำขอที่สร้างขึ้น เพื่อทำให้ระบบไฟร์วอลล์เกิดข้อผิดพลาดและอุปกรณ์อาจไม่สามารถให้บริการได้ (Denial of Service: DoS)

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้ผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการอัปเดต Security Patch ของอุปกรณ์ SonicWall ให้เป็นเวอร์ชันล่าสุดตามคำแนะนำของผู้ผลิต (SonicOS 6.5.5.5-5-28n, 7.3.2-7010 และ 8.2.0-8009) และทบทวนการกำหนดสิทธิ์การเข้าถึงระบบ พร้อมทั้งตรวจสอบระบบเพื่อค้นหาสัญญาณของการถูกบุกรุก รวมถึงเฝ้าระวังและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง และปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคามล่าสุด

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

ข้อมูลอ้างอิง

1. https://www.sonicwall.com/support/notices/security-advisory-firmware-update-required-gen-6-gen-7-and-gen-8-firewalls/kA1VN000001F03x0AC
2. https://securityaffairs.com/191527/security/sonicwall-patches-three-sonicos-flaws-in-gen-6-7-and-8-firewalls-patch-them-now.html
3. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004
4. https://nvd.nist.gov/vuln/detail/CVE-2026-0204
5. https://nvd.nist.gov/vuln/detail/CVE-2026-0205
6. https://nvd.nist.gov/vuln/detail/CVE-2026-0206