แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [ ] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ SonicWall (CVE-2024-40766)

**วันที่แจ้งเตือน 9 กันยายน 2567**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

บริษัท SonicWall ผู้ให้บริการโซลูชั่นการรักษาความปลอดภัยทางไซเบอร์ และจำหน่ายอุปกรณ์ไฟร์วอลล์ ได้เผยแพร่ช่องโหว่ระดับวิกฤต (CVE-2024-40766) ของระบบปฏิบัติการ SonicOS (ในส่วนของฟีเจอร์ management access และ SSLVPN) ซึ่งส่งผลให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบได้โดยไม่ได้รับอนุญาต และ ส่งผลให้อุปกรณ์ไฟร์วอลล์ที่ใช้งาน SonicOS ที่มีช่องโหว่ดังกล่าวเสียหาย ส่งผลให้ไม่สามารถให้บริการได้ ซึ่งพบว่าผู้ไม่หวังดีมีการใช้งานช่องโหว่ดังกล่าวเพื่อใช้โจมตีแล้ว

อุปกรณ์ และ เวอร์ชัน ที่ระบบปฏิบัติการได้รับผลกระทบ ได้แก่

| Version | Affected | Solution |
|---|---|---|
| SOHO (Gen5 Firewalls) | 5.9.2.14-12o และ เวอร์ชันที่เก่ากว่า | Upgrade เป็น 5.9.2.14-13o |
| Gen6 Firewalls | 6.5.4.14-109n และ เวอร์ชันที่เก่ากว่า | Upgrade เป็น 6.5.2.8-2n (สำหรับ SM9800, NSsp 12400, NSsp 12800) และ Upgrade เป็น 6.5.4.15.116n (สำหรับอุปกรณ์ Gen6 Firewall อื่น ๆ) |
| Gen7 Firewalls | SonicOS build version 7.0.1-5035 และ เวอร์ชันที่เก่ากว่า | Upgrade เป็นเวอร์ชันล่าสุด |

คำแนะนำเบื้องต้นเพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ดังกล่าว (workaround) ดังนี้

1. จำกัดการเข้าถึงส่วนบริหารจัดการไฟร์วอลล์ (firewall management) โดยอนุญาตเฉพาะผู้ใช้งานที่มีสิทธิเท่านั้น และปิดการเข้าถึงจากอินเทอร์เน็ตหากเป็นไปได้
2. จำกัดการเข้าถึง SSLVPN ให้เฉพาะผู้ใช้งานหรือต้นทางที่เชื่อถือได้เท่านั้น และปิดการใช้งานหากไม่จำเป็น
3. สำหรับอุปกรณ์ Gen5 และ Gen6 Firewalls ผู้ใช้งาน SSLVPN ที่มีบัญชีในระบบ (local account) ควรแก้ไขรหัสผ่านทันที และผู้ดูแลระบบควรเปิดใช้งาน “User must change password” สำหรับผู้ใช้งาน (local account) ในระบบ
4. เปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (MFA) สำหรับผู้ใช้งาน SSLVPN โดยใช้ TOTP หรือรหัสผ่านครั้งเดียวที่ส่งทางอีเมล (OTPs) ข้อมูลเพิ่มเติมเกี่ยวกับวิธีการตั้งค่านี้สามารถดูได้ตามข้อมูลอ้างอิง 1)

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

**ข้อมูลอ้างอิง**


1) https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015
2) https://nvd.nist.gov/vuln/detail/CVE-2024-40766#VulnChangeHistorySection
3) https://www.bleepingcomputer.com/news/security/sonicwall-sslvpn-access-control-flaw-is-now-exploited-in-attacks/