

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability



แจ้งเตือน กรณีพบการโจมตี Cloud Backup Service ของผลิตภัณฑ์ SonicWall

วันที่แจ้งเตือน 26 กันยายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีผู้ไม่หวังดีสามารถเข้าถึงไฟล์การตั้งค่าสำรอง (Backup Firewall Preference Files) ของ SonicWall Firewall ที่เก็บไว้บนระบบ Cloud แม้ว่าข้อมูล Credentials ที่อยู่ในไฟล์เหล่านี้จะถูกเข้ารหัสไว้ แต่ยังมีข้อมูลอื่น ๆ ที่ผู้ไม่หวังดีสามารถนำไปใช้ประโยชน์ในการโจมตีระบบได้ ซึ่งอาจก่อให้เกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลสำคัญ เช่น Credentials และ Tokens ที่ใช้กับบริการต่าง ๆ บนอุปกรณ์ SonicWall Firewall ภายในเครือข่าย เป็นต้น และอาจนำไปสู่ความเสี่ยงด้านความมั่นคงปลอดภัยขององค์กรได้

ผลิตภัณฑ์ที่ได้รับผลกระทบ:

อุปกรณ์ SonicWall Firewalls ที่มีการสำรองไฟล์การตั้งค่าไว้บนเว็บไซต์ MySonicWall.com

แนวทางการตรวจสอบและป้องกันกรณีใช้ผลิตภัณฑ์ดังกล่าว:

- เข้าสู่ระบบ MySonicWall.com และตรวจสอบว่ามีไฟล์ Cloud Backup สำหรับอุปกรณ์ Firewall หรือไม่
 - หากไม่มีการสำรองข้อมูลไว้บน Cloud หมายความว่า Firewall ของท่านไม่ได้รับผลกระทบ
 - หากมีการสำรองข้อมูลไว้บน Cloud ให้ทำการตรวจสอบว่า Serial Number ของอุปกรณ์ ถูกระบุอยู่ใน Product Management | Issue List หรือไม่
- หากพบว่า Serial Number ของอุปกรณ์ถูกติด Flag ไว้ (ติด Flagged ไว้ด้วย Name, Last Download Date และ Known Impacted Services) แสดงว่า Serial Number นั้นมีความเสี่ยงและควรปฏิบัติตามแนวทางการดำเนินการที่ SonicWall แนะนำ (อ้างอิง 2)
- หากเคยใช้ฟีเจอร์ Cloud Backup ควรติดตามคำแนะนำเพิ่มเติมจาก SonicWall (อ้างอิง 3)

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 25 ก.ย. 2568
- <https://www.sonicwall.com/support/knowledge-base/essential-credential-reset/250909151701590>
- <https://www.sonicwall.com/support/knowledge-base/mysonicwall-cloud-backup-file-incident/250915160910330>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ