วันที่ 15 ตุลาคม 2568

ผู้เชี่ยวชาญเตือนถึงการถูกโจมตีครั้งใหญ่ของ SonicWall VPN ที่ส่งผลกระทบต่อบัญชีกว่า 100 บัญชี

บริษัทด้านความปลอดภัยไซเบอร์ Huntress ออกมาเตือนเมื่อวันศุกร์ถึงสถานการณ์ “การโจมตีในวงกว้าง” ที่เกิดขึ้นกับอุปกรณ์ SonicWall SSL VPN ซึ่งองค์กรต่าง ๆ ใช้เพื่อเข้าถึงระบบของลูกค้าหลายราย

Huntress ระบุว่า "กลุ่มผู้ไม่หวังดีสามารถล็อกอินเข้าสู่บัญชีจำนวนมากได้อย่างรวดเร็วผ่านอุปกรณ์ที่ถูกเจาะ" และเน้นย้ำถึงกลไกการโจมตีว่า "ความเร็วและขอบเขตของการโจมตีในครั้งนี้บ่งชี้ว่า แฮ็กเกอร์น่าจะมีรหัสผ่านที่ถูกต้องอยู่แล้วมากกว่าจะเป็นการสุ่มเดารหัส (brute-force)"

ขอบเขตการโจมตี การสแกนเครือข่าย และที่มาของ IP

- ขอบเขต: การโจมตีส่วนใหญ่เริ่มขึ้นตั้งแต่วันที่ 4 ตุลาคม 2025 โดยมีบัญชี SonicWall SSL VPN มากกว่า 100 บัญชี ในลูกค้า 16 ราย ที่ได้รับผลกระทบ
- ที่มา: จากการตรวจสอบของ Huntress พบว่าการล็อกอินเข้าสู่ระบบ SonicWall เหล่านี้มีต้นทางมาจาก IP address 202.155.8[.]73

พฤติกรรมหลังการเจาะเครือข่าย:

- บริษัทระบุเพิ่มเติมว่า ในบางกรณีแฮ็กเกอร์ไม่ได้ทำกิจกรรมอื่นใดภายในเครือข่าย และจะตัดการเชื่อมต่อออกหลังจากอยู่ในระบบเพียงไม่นาน
- แต่ในบางกรณี พวกเขากลับทำการสแกนเครือข่าย และพยายามเข้าถึงบัญชี Windows ภายในระบบหลายบัญชี

ความเสี่ยงคู่ขนาน: ไฟล์สำรอง MySonicWall รั่วไหล

การเปิดเผยเรื่องการโจมตี VPN นี้เกิดขึ้นหลังจาก SonicWall ยอมรับว่าเกิดเหตุด้านความปลอดภัย ทำให้ไฟล์สำรองการตั้งค่าของไฟร์วอลล์ที่เก็บไว้ในบัญชี MySonicWall ถูกเปิดเผยโดยไม่ได้รับอนุญาต เหตุการณ์นี้ส่งผลกระทบต่อผู้ใช้ทุกคนที่เคยใช้บริการสำรองข้อมูลบนคลาวด์ของ SonicWall

Arctic Wolf บริษัทด้านความปลอดภัย กล่าวเสริมว่า "ไฟล์การตั้งค่าไฟร์วอลล์เก็บข้อมูลสำคัญที่อาจถูกนำไปใช้โดยผู้ไม่หวังดีเพื่อเจาะเข้าและเข้าถึงเครือข่ายขององค์กรได้" "ไฟล์เหล่านี้สามารถให้ข้อมูลสำคัญแก่ผู้โจมตี เช่น การตั้งค่าผู้ใช้ กลุ่ม และโดเมนการตั้งค่า DNS และ log รวมถึงใบรับรองต่างๆ"

อย่างไรก็ตาม Huntress ระบุว่า ณ ตอนนี้ยังไม่มีหลักฐานที่เชื่อมโยงเหตุไฟล์รั่วดังกล่าวกับการโจมตี SonicWall SSL VPN ที่เพิ่มขึ้นในช่วงนี้

คำแนะนำเร่งด่วนเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

เนื่องจากไฟล์การตั้งค่าไฟร์วอลล์มักมีข้อมูลรหัสผ่านที่สำคัญ องค์กรที่ใช้บริการสำรองข้อมูลผ่าน MySonicWall ควรรีเซ็ตรหัสผ่านบนอุปกรณ์ไฟร์วอลล์ที่ใช้งานอยู่ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

นอกจากนี้ ยังมีคำแนะนำดังนี้:

1. จำกัดการจัดการผ่าน WAN และการเข้าถึงจากระยะไกลในกรณีที่ไม่จำเป็น
2. ยกเลิกคีย์ API ภายนอกที่เกี่ยวข้องกับไฟร์วอลล์หรือระบบจัดการ
3. ตรวจสอบการล็อกอินที่อาจน่าสงสัย
4. เปิดใช้ระบบยืนยันตัวตนหลายชั้น (MFA) สำหรับบัญชีผู้ดูแลและการเข้าถึงจากระยะไกลทั้งหมด

ภัยมัลแวร์เรียกค่าไถ่ Akira: การใช้ช่องโหว่ที่รู้จักแล้ว

การเปิดเผยนี้เกิดขึ้นท่ามกลางการเพิ่มขึ้นของการโจมตีเรียกค่าไถ่ (ransomware) ที่มุ่งเป้าไปยังอุปกรณ์ไฟร์วอลล์ของ SonicWall โดยใช้ ช่องโหว่ที่รู้จักแล้ว (CVE-2024-40766) เพื่อเจาะเข้าสู่เครือข่ายเป้าหมายและติดตั้งมัลแวร์เรียกค่าไถ่ Akira

รายงานจาก Darktrace ที่เผยแพร่ในสัปดาห์นี้ระบุว่า มีการตรวจพบการบุกรุกต่อองค์กรในสหรัฐฯ รายหนึ่งเมื่อช่วงปลายเดือนสิงหาคม 2025 ซึ่งเกี่ยวข้องกับ:

- การสแกนเครือข่าย การเก็บข้อมูลภายใน
- การเคลื่อนย้ายสิทธิ์ภายในระบบ
- การยกระดับสิทธิ์ผู้ใช้ผ่านเทคนิคอย่าง “UnPAC the hash”
- และการขโมยข้อมูลออกจากระบบ

"อุปกรณ์หนึ่งที่ถูกโจมตีในเหตุการณ์นี้ถูกระบุภายหลังว่าเป็น เซิร์ฟเวอร์ SonicWall VPN ซึ่งบ่งชี้ว่าการโจมตีดังกล่าวเป็นส่วนหนึ่งของแคมเปญมัลแวร์เรียกค่าไถ่ Akira ที่มุ่งเป้าไปยังเทคโนโลยีของ SonicWall" รายงานระบุ

บทสรุปและคำเตือน: "แคมเปญของกลุ่ม Akira แสดงให้เห็นถึงความสำคัญอย่างยิ่งของการอัปเดตแพตช์อย่างสม่ำเสมอ แฮ็กเกอร์ยังคงใช้ช่องโหว่ที่เปิดเผยแล้ว ไม่ใช่เฉพาะช่องโหว่ใหม่ ๆ เท่านั้น ซึ่งตอกย้ำถึงความจำเป็นของการเฝ้าระวังอย่างต่อเนื่อง แม้จะมีการปล่อยแพตช์แก้ไขออกมาแล้วก็ตาม" นี่คือข้อสรุปที่เน้นย้ำถึงความเร่งด่วนในการดูแลความปลอดภัยของอุปกรณ์เครือข่ายที่เข้าถึงจากภายนอก.

ข้อมูลอ้างอิง

Oct 11, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/10/experts-warn-of-widespread-sonicwall.html