วันที่ 8 สิงหาคม 2568

SonicWall ยืนยันช่องโหว่ที่ถูกแพตช์แล้วเป็นสาเหตุของการโจมตี VPN ล่าสุด ไม่ใช่ Zero-Day

เมื่อไม่นานมานี้มีรายงานถึงการโจมตีที่เพิ่มขึ้นอย่างน่าเป็นห่วง ซึ่งพุ่งเป้าไปที่ไฟร์วอลล์ SonicWall Gen 7 และรุ่นใหม่กว่าที่เปิดใช้งาน SSL VPN ทำให้หลายฝ่ายกังวลว่าอาจมีช่องโหว่ Zero-Day ใหม่ถูกค้นพบ

แต่ล่าสุด SonicWall ได้ออกมาให้ความกระจ่างแล้วว่า การโจมตีที่เกิดขึ้นนั้นไม่ได้เชื่อมโยงกับช่องโหว่ Zero-Day แต่กลับมีความเกี่ยวข้องกับช่องโหว่เก่าที่ได้รับการแพตช์ไปแล้ว และปัญหาจากการนำรหัสผ่านเก่ากลับมาใช้ซ้ำ

“ตอนนี้เรามีความมั่นใจอย่างสูงว่ากิจกรรมที่เกี่ยวข้องกับ SSL VPN ที่เกิดขึ้นเมื่อเร็วๆ นี้ ไม่ได้เชื่อมโยงกับช่องโหว่ Zero-Day” บริษัทกล่าว “แต่กลับมีความเชื่อมโยงอย่างมีนัยสำคัญกับกิจกรรมที่เกี่ยวข้องกับช่องโหว่หมายเลข CVE-2024-40766”

เจาะลึกช่องโหว่ CVE-2024-40766

CVE-2024-40766 (คะแนน CVSS: 9.3) ถูกเปิดเผยครั้งแรกโดย SonicWall ในเดือนสิงหาคม 2024 โดยระบุว่าเป็นปัญหาการควบคุมสิทธิ์เข้าถึงที่ไม่เหมาะสม ซึ่งอาจเปิดช่องให้ผู้ไม่หวังดีสามารถเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

“ช่องโหว่ด้านการควบคุมการเข้าถึงที่ไม่เหมาะสมถูกตรวจพบในระบบจัดการของ SonicWall SonicOS ซึ่งอาจทำให้มีการเข้าถึงทรัพยากรโดยไม่ได้รับอนุญาต และในบางกรณีอาจทำให้ไฟร์วอลล์ล่มได้” บริษัทระบุไว้ในประกาศ ณ เวลานั้น

SonicWall ยังกล่าวเพิ่มเติมว่า ขณะนี้กำลังสืบสวนเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมดังกล่าวซึ่งมีน้อยกว่า 40 เหตุการณ์ และหลายเหตุการณ์นั้นเกี่ยวข้องกับการย้ายระบบจากไฟร์วอลล์ Gen 6 ไปยัง Gen 7 โดยไม่ได้มีการรีเซ็ตรหัสผ่านของผู้ใช้งานภายใน ซึ่งถือเป็นคำแนะนำที่สำคัญในการรับมือช่องโหว่ CVE-2024-40766

นอกจากนี้ บริษัทยังชี้ว่า SonicOS 7.3 มีระบบป้องกันเพิ่มเติมต่อการโจมตีแบบเดารหัสผ่านซ้ำๆ (Brute-force) และการโจมตีระบบยืนยันตัวตนแบบหลายปัจจัย (MFA)

คำแนะนำล่าสุดเพื่อป้องกันภัย

เพื่อความปลอดภัยสูงสุดและป้องกันการโจมตีจากช่องโหว่เก่าและรหัสผ่านที่ถูกนำมาใช้ซ้ำ SonicWall ได้ให้คำแนะนำดังนี้:

- อัปเดตเฟิร์มแวร์เป็น SonicOS เวอร์ชัน 7.3.0
- รีเซ็ตรหัสผ่านของผู้ใช้ทั้งหมด ที่มีสิทธิ์เข้าถึง SSLVPN โดยเฉพาะบัญชีที่ถูกย้ายมาจาก Gen 6 ไปยัง Gen 7
- เปิดใช้งานระบบป้องกัน Botnet และการกรองตามตำแหน่งทางภูมิศาสตร์ (Geo-IP Filtering)
- บังคับใช้ MFA และนโยบายการตั้งรหัสผ่านที่รัดกุม
- ลบบัญชีผู้ใช้ที่ไม่ได้ใช้งานหรือไม่มีความเคลื่อนไหว

การพัฒนานี้เกิดขึ้นในขณะที่มีผู้ให้บริการด้านความปลอดภัยหลายแห่งรายงานว่า พบการเพิ่มขึ้นของการโจมตีที่อาศัยช่องโหว่ใน SonicWall SSL VPN เพื่อนำไปใช้โจมตีด้วย Akira ransomware ซึ่งเน้นย้ำว่าแม้จะเป็นช่องโหว่เก่าแต่หากไม่ได้รับการแก้ไขอย่างถูกต้องก็ยังคงเป็นภัยคุกคามร้ายแรงได้

ข้อมูลอ้างอิง

Aug 7, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/08/sonicwall-confirms-patched.html