วันที่ 11 พฤษภาคม 2569

ช่องโหว่ PAN-OS แบบ RCE ถูกนำไปใช้โจมตีจริง เปิดทางให้ยึดสิทธิ์ Root และใช้ในการขโมยข้อมูล

Palo Alto Networks เปิดเผยว่า มีความเป็นไปได้ที่ผู้ไม่หวังดีได้พยายามใช้ประโยชน์จากช่องโหว่ความปลอดภัยระดับร้ายแรงที่เพิ่งมีการเปิดเผยออกมา โดยพบความพยายามดังกล่าวตั้งแต่วันที่ 9 เมษายน 2026

ช่องโหว่นี้มีรหัสว่า CVE-2026-0300 (คะแนน CVSS 9.3/8.7) เป็นช่องโหว่ประเภท Buffer Overflow ในบริการUser-ID Authentication Portal ของซอฟต์แวร์ PAN-OS ซึ่งอาจเปิดโอกาสให้ผู้โจมตีจากภายนอกที่ไม่ต้องยืนยันตัวตน สามารถรันคำสั่งที่ต้องการด้วยสิทธิ์ระดับ Root ได้ เพียงแค่ส่งแพ็กเก็ตที่ถูกสร้างขึ้นมาเป็นพิเศษไปยังระบบ

คำแนะนำในการแก้ไขและป้องกันชั่วคราว

อัปเดตแก้ไขช่องโหว่นี้จะเริ่มเผยแพร่ตั้งแต่ 13 พฤษภาคม 2026 เป็นต้นไป แต่ระหว่างรอแพตช์ Palo Alto Networks แนะนำให้องค์กรดำเนินการดังนี้ทันที

- จำกัดการเข้าถึง PAN-OS User-ID Authentication Portal ให้เฉพาะเครือข่ายหรือโซนที่เชื่อถือได้ ปิดการใช้งาน Portal นั้นทิ้งเลย หากองค์กรไม่ได้ใช้งาน
- ปิดฟังก์ชัน Response Pages ใน Interface Management Profile สำหรับทุก L3 Interface ที่รับทราฟฟิกจากอินเทอร์เน็ตหรือเครือข่ายที่ไม่น่าเชื่อถือ
- สำหรับลูกค้าที่ใช้ Advanced Threat Prevention ให้เปิด Threat ID 510019 จากชุดอัปเดต Applications and Threats content เวอร์ชัน 9097-10022 เพื่อบล็อกการโจมตีได้ทันที

รายละเอียดการโจมตีโดยกลุ่ม CL-STA-1132

ในประกาศแจ้งเตือนที่เผยแพร่เมื่อวันพุธที่ผ่านมา บริษัทระบุว่า ได้รับทราบถึงการโจมตีจริงในวงจำกัด และกำลังติดตามกิจกรรมดังกล่าวภายใต้ชื่อ CL-STA-1132 ซึ่งเชื่อว่าเป็นกลุ่มผู้โจมตีที่ได้รับการสนับสนุนจากรัฐ แต่ยังไม่สามารถระบุแหล่งที่มาได้อย่างชัดเจน

Unit 42 ระบุว่า ผู้โจมตีที่อยู่เบื้องหลังกิจกรรมนี้ใช้ช่องโหว่CVE-2026-0300 เพื่อให้สามารถรันโค้ดจากระยะไกล (RCE)บน PAN-OS ได้โดยไม่ต้องยืนยันตัวตน เมื่อโจมตีสำเร็จ ผู้โจมตีสามารถฝัง Shellcode เข้าไปในโปรเซสnginx worker ได้

บริษัทด้านความมั่นคงปลอดภัยไซเบอร์แห่งนี้ระบุว่า พบความพยายามโจมตีที่ไม่สำเร็จต่ออุปกรณ์ PAN-OS ตั้งแต่วันที่ 9 เมษายน 2026 และหลังจากนั้นประมาณหนึ่งสัปดาห์ ผู้โจมตีสามารถเจาะระบบได้สำเร็จและฝัง Shellcode ลงในอุปกรณ์ทันทีที่ได้สิทธิ์เข้าถึงระบบ ผู้โจมตีได้ลบร่องรอยต่างๆ เช่น การลบข้อความ crash ใน kernel การลบข้อมูล crashของ nginx และการลบไฟล์ core dump เพื่อปกปิดการบุกรุก

หลังจากเข้าควบคุมระบบแล้ว ผู้โจมตีได้ดำเนินกิจกรรมเพิ่มเติม เช่น การสำรวจข้อมูลใน Active Directory (AD) และติดตั้งเครื่องมือเพิ่มเติมอย่าง EarthWorm และ ReverseSocks5 ลงบนอุปกรณ์อีกเครื่องหนึ่งเมื่อวันที่29 เมษายน 2026 เครื่องมือทั้งสองนี้เคยถูกพบว่าใช้งานโดยกลุ่มแฮกเกอร์หลายกลุ่มที่มีความเชื่อมโยงกับประเทศจีน

พฤติกรรมและเทคนิคของกลุ่มผู้โจมตีระดับรัฐ

Unit 42 ระบุเพิ่มเติมว่า ตลอดช่วงห้าปีที่ผ่านมา กลุ่มผู้โจมตีระดับรัฐที่มุ่งเน้นการจารกรรมข้อมูล ได้หันมาให้ความสำคัญกับอุปกรณ์เครือข่ายที่อยู่บริเวณรอบระบบมากขึ้น เช่น ไฟร์วอลล์ เราเตอร์ อุปกรณ์ IoT ไฮเปอร์ไวเซอร์ และระบบ VPNต่างๆ เนื่องจากอุปกรณ์เหล่านี้มีสิทธิ์การเข้าถึงระดับสูง แต่โดยทั่วไปมักไม่มีระบบบันทึกข้อมูลและเครื่องมือรักษาความปลอดภัยที่ครบถ้วนเหมือนกับคอมพิวเตอร์ทั่วไป

การที่ผู้โจมตีในกลุ่ม CL-STA-1132 เลือกใช้เครื่องมือแบบโอเพนซอร์สแทนการพัฒนามัลแวร์ของตนเอง ช่วยลดโอกาสที่จะถูกตรวจจับด้วยระบบที่อาศัยลายเซ็นของมัลแวร์ อีกทั้งยังทำให้สามารถแทรกตัวเข้ากับสภาพแวดล้อมขององค์กรได้อย่างแนบเนียน นอกจากนี้ พวกเขายังใช้รูปแบบการปฏิบัติการที่มีระเบียบ โดยเชื่อมต่อเข้ามาเป็นช่วงๆ ตลอดหลายสัปดาห์ เพื่อหลีกเลี่ยงไม่ให้พฤติกรรมดังกล่าวเกินระดับที่ระบบแจ้งเตือนอัตโนมัติส่วนใหญ่จะตรวจจับได้

ข้อมูลอ้างอิง

May 7, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/05/pan-os-rce-exploit-under-active-use.html