

วันที่ 16 ตุลาคม 2569

Palo Alto Networks ออกแพตช์แก้ไขช่องโหว่ RCE ใน PAN-OS หลังพบว่าถูกนำไปใช้โจมตีแล้ว



Palo Alto Networks ออกอัปเดตด้านความปลอดภัยเมื่อวันพุธที่ผ่านมา เพื่อแก้ไขช่องโหว่ระดับความรุนแรงสูงในซอฟต์แวร์ PAN-OS หลังพบว่าช่องโหว่ดังกล่าวกำลังถูกนำไปใช้โจมตีจริง ช่องโหว่นี้มีรหัส CVE-2026-0322 (คะแนน CVSS 8.6) เป็นช่องโหว่ประเภท Remote Code Execution (RCE) ซึ่งเปิดโอกาสให้ผู้โจมตีสามารถส่งรันโค้ดจากระยะไกลผ่านหน้าจัดการระบบได้ โดยช่องโหว่ Remote Code Execution (RCE) ในหน้าจัดการระบบของซอฟต์แวร์ PAN-OS ทำให้ผู้โจมตีที่ผ่านการยืนยันตัวตนแล้ว และสามารถเชื่อมต่อเครือข่ายไปยังหน้าจัดการระบบ สามารถส่งรันโค้ดใดๆ บนอุปกรณ์ไฟร์วอลล์ด้วยสิทธิ์ระดับสูงสุด (root) ได้

ช่องโหว่นี้ส่งผลกระทบต่ออุปกรณ์ไฟร์วอลล์ที่ใช้ซอฟต์แวร์ PAN-OS ทั้งรุ่น PA-Series และ VM-Series รวมถึงระบบบริหารจัดการ Panorama ทั้งแบบ Virtual และ M-Series อย่างไรก็ตาม ผลิตภัณฑ์ Cloud NGFW และ Prisma Access ไม่ได้รับผลกระทบจากช่องโหว่นี้ Palo Alto Networks ยังระบุว่า ผู้โจมตีไม่จำเป็นต้องอาศัยการตั้งค่าพิเศษใดๆ เพื่อใช้ประโยชน์จากช่องโหว่นี้ แต่ผู้ดูแลระบบสามารถลดความเสี่ยงได้ด้วยการจำกัดการเข้าถึงหน้าจัดการระบบ โดยอนุญาตให้เฉพาะ IP Address ภายในองค์กรที่เชื่อถือได้เท่านั้น

บริษัทได้อธิบายเพิ่มเติมว่า "คุณสามารถลดความเสี่ยงจากการถูกโจมตีได้ด้วยการกำหนดให้เข้าถึงหน้าจัดการระบบผ่าน Jump Box เท่านั้น โดยให้ Jump Box เป็นระบบเพียงเครื่องเดียวที่ได้รับอนุญาตให้เชื่อมต่อกับหน้าจัดการระบบได้"

ขณะนี้แพตช์แก้ไขช่องโหว่สำหรับ PAN-OS ในเวอร์ชันต่อไปนี้

- PAN-OS: ตั้งแต่เวอร์ชัน 12.2.4 ขึ้นไป
- PAN-OS: ตั้งแต่เวอร์ชัน 12.1.4-h12, 12.1.7-h8, 12.1.10-h2 ขึ้นไป
- PAN-OS: ตั้งแต่เวอร์ชัน 11.2.4-h22, 11.2.7-h21, 11.2.10-h15, 11.2.13-h3, 11.2.16 ขึ้นไป (คาดว่าจะพร้อมใช้งานวันที่ 15 ตุลาคม 2026)
- PAN-OS: ตั้งแต่เวอร์ชัน 11.1.4-h37, 11.1.6-h39, 11.1.7-h11, 11.1.10-h35, 11.1.13-h15, 11.1.16-h3 ขึ้นไป

- PAN-OS: ตั้งแต่เวอร์ชัน 10.2.7-h38, 10.2.10-h41, 10.2.13-h26, 10.2.16-h11, 10.2.18-h12 ขึ้นไป

Palo Alto Networks ยืนยันว่า พบความพยายามโจมตีผ่านช่องโหว่ที่มุ่งเป้าไปยังหน้าจัดการระบบของอุปกรณ์ Palo Alto Networks แล้ว แต่ยังพบในจำนวนที่จำกัดมาก อย่างไรก็ตาม บริษัทยังไม่ได้เปิดเผยรายละเอียดเกี่ยวกับรูปแบบการโจมตี ผู้ที่อยู่เบื้องหลัง หรือช่วงเวลาที่มีการโจมตีเริ่มต้นขึ้น

สำหรับ IP Address ที่ตรวจพบที่มีความเชื่อมโยงกับความพยายามโจมตีช่องโหว่นี้ และมีตำแหน่งที่ตั้งอยู่ในสหรัฐอเมริกา มีดังต่อไปนี้

- 66.42.72[.]14
- 208.83.239[.]114
- 149.248.47[.]234

บริษัทได้กล่าวขอบคุณ Suraj Siddharudh นักวิจัยด้านความปลอดภัยผลิตภัณฑ์ระดับอาวุโสของ Palo Alto Networks ซึ่งเป็นผู้ค้นพบและรายงานช่องโหว่นี้

การเปิดเผยช่องโหว่ดังกล่าวเกิดขึ้นในช่วงเวลาเดียวกับที่ Cisco ออกมาเตือนว่า กลุ่มผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ระดับวิกฤตใน Cisco Secure Email Gateway ซึ่งมีรหัส CVE-2026-76519 (คะแนน CVSS 9.8) โดยช่องโหว่นี้อาจทำให้ผู้โจมตีจากระยะไกลที่ไม่จำเป็นต้องผ่านการยืนยันตัวตน สามารถเขียนไฟล์ใดๆ ลงในระบบปฏิบัติการของอุปกรณ์ที่ได้รับผลกระทบได้

Cisco อธิบายว่า "ช่องโหว่นี้เกิดจากการจัดการไฟล์แนบอีเมลที่ไม่เหมาะสม ในกรณีที่เปิดใช้งานบริการตรวจสอบความน่าเชื่อถือของไฟล์ (File Reputation Service) โดยผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นี้ด้วยการส่งอีเมลที่มีไฟล์แนบซึ่งถูกสร้างขึ้นเป็นพิเศษผ่านอุปกรณ์ที่ได้รับผลกระทบ หากโจมตีสำเร็จ ผู้โจมตีอาจสามารถเขียนไฟล์ใดๆ และสั่งรันคำสั่งบนระบบปฏิบัติการของอุปกรณ์ด้วยสิทธิ์ระดับสูงสุด (root) ได้"

ล่าสุด สำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐอเมริกา (CISA) ได้เพิ่มช่องโหว่ทั้ง CVE-2026-0322 และ CVE-2026-76519 ลงในบัญชีช่องโหว่ที่พบว่าถูกนำไปใช้โจมตีจริง หรือ Known Exploited Vulnerabilities (KEV) พร้อมกำหนดให้หน่วยงานพลเรือนของรัฐบาลกลางสหรัฐฯ (FCEB) เร่งดำเนินการแก้ไขช่องโหว่เหล่านี้ภายในวันที่ 17 ตุลาคม 2026

ข้อมูลอ้างอิง

Oct 15, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/10/palo-alto-networks-patches-pan-os.html>