แจ้งเตือน

Alert

**ผลกระทบทางธุรกิจ**

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

**ผลกระทบต่อระบบ**

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# Palo Alto ออก Security Patch แก้ไขช่องโหว่ CVE-2026-0300

**วันที่แจ้งเตือน 7 พฤษภาคม 2569**

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Palo Alto Networks ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ (CVE-2026-0300) ในระบบปฏิบัติการ PAN-OS (ในบางเวอร์ชั่นของ PAN-OS 10.2, PAN-OS 11.1, PAN-OS 11.2 และ PAN-OS 12.1) ที่เกี่ยวข้องกับอุปกรณ์ไฟร์วอลล์ ซึ่งถูกนำไปใช้ในการโจมตีจริง

ช่องโหว่ดังกล่าวเป็นช่องโหว่ buffer overflow vulnerability ในบริการ User-ID Authentication Portal ทำให้ผู้ไม่หวังดีใช้เพื่อส่งคำขอที่ถูกสร้างขึ้นเข้าสู่ระบบจากระยะไกลโดยใช้สิทธิ Root ได้ เป็นผลให้ผู้ไม่หวังดีเข้าควบคุม จัดการการตั้งค่า หรือเข้าถึงข้อมูลสำคัญภายในเครือข่ายขององค์กรได้ และอาจถูกใช้เพื่อเปลี่ยนแปลงนโยบายด้านความปลอดภัย สร้างบัญชีผู้ใช้งานใหม่ หรือฝังโค้ดอันตรายในอุปกรณ์ไฟร์วอลล์ ส่งผลให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบเครือข่ายและการดำเนินงานขององค์กร

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้ผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่ผู้ผลิตได้แก้ไขช่องโหว่แล้ว และทบทวนการเปิดใช้งานการเข้าถึง Interface จากเครือข่ายภายนอก ควบคู่กับการเฝ้าระวังสถานะการทำงานของอุปกรณ์ไฟร์วอลล์และปริมาณทราฟฟิกที่ผิดปกติ รวมทั้งจัดเตรียมแผนรองรับกรณีเกิดเหตุการณ์หยุดชะงักของระบบ เพื่อให้สามารถฟื้นฟูการให้บริการได้อย่างทันท่วงที

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท


**ข้อมูลอ้างอิง**

1. https://thehackernews.com/2026/05/palo-alto-pan-os-flaw-under-active.html
2. https://security.paloaltonetworks.com/CVE-2026-0300
3. https://www.hkcert.org/security-bulletin/palo-alto-pan-os-remote-code-execution-vulnerability_20260506