

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

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



Palo Alto Networks แจ้งเตือนการโจมตีผ่านช่องโหว่ PAN-OS (CVE-2025-0108)

วันที่แจ้งเตือน 18 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบการธุรกิจหลักทรัพย์และผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ และพบการรายงานช่องโหว่ในผลิตภัณฑ์ Palo Alto Networks PAN-OS Firewalls (CVE-2025-0108) ซึ่งทำให้ผู้ไม่ประสงค์ดีสามารถหลบเลี่ยงระบบยืนยันตัวตน (Authentication Bypass) และเรียกใช้สคริปต์ PHP ที่เป็นอันตราย โดยอาจส่งผลให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลสำคัญของระบบ เปลี่ยนแปลงการตั้งค่าของ Firewalls ที่จะส่งผลกระทบต่อความปลอดภัยของระบบเครือข่าย และอาจนำไปสู่การโจมตีในรูปแบบอื่น ๆ ที่มีความรุนแรงมากขึ้น

ทั้งนี้ Palo Alto Networks แนะนำให้ผู้ใช้งานอัปเดต PAN-OS เป็นเวอร์ชันต่าง ๆ ดังนี้

| PAN-OS | เวอร์ชันซอฟต์แวร์ |
|-------------|------------------------|
| PAN-OS 11.2 | 11.2.4-h4 หรือสูงกว่า |
| PAN-OS 11.1 | 11.1.6-h1 หรือสูงกว่า |
| PAN-OS 10.2 | 10.2.13-h3 หรือสูงกว่า |
| PAN-OS 10.1 | 10.1.14-h9 หรือสูงกว่า |

กรณี ผู้ประกอบการธุรกิจที่ใช้ผลิตภัณฑ์ดังกล่าว ควรพิจารณาดำเนินการอัปเดต PAN-OS Firewalls ตามที่ Palo Alto Network และควรเพิ่มมาตรการ เพื่อควบคุมการเข้าถึง PAN-OS management web interface ของ Firewall ดังกล่าว รวมถึงตรวจสอบ Log อย่างสม่ำเสมอ เพื่อปรับปรุงระบบตรวจจับการบุกรุกให้มีประสิทธิภาพอยู่เสมอและเพื่อให้สามารถตรวจจับการโจมตีได้ รวมทั้งติดตามข่าวสารและประกาศเตือนภัยเกี่ยวกับช่องโหว่และความเสี่ยงทางไซเบอร์อย่างใกล้ชิด เพื่อประกอบการพิจารณาดำเนินการตามความเหมาะสมต่อไป

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบการธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบการธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

- <https://www.bleepingcomputer.com/news/security/hackers-exploit-authentication-bypass-in-palo-alto-networks-pan-os/>
- <https://securityaffairs.com/174237/hacking/exploitation-palo-alto-networks-pan-os-firewalls-bug.html>
- <https://security.paloaltonetworks.com/CVE-2025-0108>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ