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 Network ออก Security Patch แก้ไขช่องโหว่ในผลิตภัณฑ์ GlobalProtect Firewall และ Portal (CVE-2026-0227)

วันที่แจ้งเตือน 16 มกราคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Palo Alto Networks ได้ออกอัปเดตด้านความมั่นคงปลอดภัยเพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์ Palo Alto GlobalProtect Firewall และ Portal (CVE-2026-0227) ที่ผู้ไม่ประสงค์ดีอาจใช้ช่องโหว่นี้โจมตีแบบ Denial of Service (DoS) ต่ออุปกรณ์ไฟร์วอลล์ ทำให้การรับส่งข้อมูลเครือข่ายและการทำงานของระบบป้องกันหยุดชะงักได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้ผลิตภัณฑ์ Palo Alto GlobalProtect Firewall และ Portal พิจารณาดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่ผู้ผลิตได้แก้ไขช่องโหว่แล้ว และทบทวนการเปิดใช้งาน ควบคู่กับการเฝ้าระวังสถานะการทำงานของอุปกรณ์ไฟร์วอลล์และปริมาณทราฟฟิกที่ผิดปกติ รวมทั้งจัดเตรียมแผนรองรับกรณีเกิดเหตุการณ์หยุดชะงักของระบบ เพื่อให้สามารถฟื้นฟูการให้บริการได้อย่างทันท่วงที

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 12.1	< 12.1.3-h3 < 12.1.4	>= 12.1.3-h3 >= 12.1.4
PAN-OS 11.2	< 11.2.4-h15 < 11.2.7-h8 < 11.2.10-h2	>= 11.2.4-h15 (ETA: 1/14/2026) >= 11.2.7-h8 >= 11.2.10-h2
PAN-OS 11.1	< 11.1.4-h27 < 11.1.6-h23 < 11.1.10-h9 < 11.1.13	>= 11.1.4-h27 >= 11.1.6-h23 >= 11.1.10-h9 >= 11.1.13
PAN-OS 10.2	< 10.2.7-h32 < 10.2.10-h30 < 10.2.13-h18 < 10.2.16-h6 < 10.2.18-h1	>= 10.2.7-h32 >= 10.2.10-h30 >= 10.2.13-h18 >= 10.2.16-h6 >= 10.2.18-h1
PAN-OS 10.1	< 10.1.14-h20	>= 10.1.14-h20
Prisma Access 11.2	< 11.2.7-h8*	>= 11.2.7-h8*
Prisma Access 10.2	< 10.2.10-h29*	>= 10.2.10-h29*

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

ข้อมูลอ้างอิง

1. https://securityaffairs.com/186948/hacking/palo-alto-networks-addressed-a-globalprotect-flaw-poc-exists.html
2. https://nvd.nist.gov/vuln/detail/CVE-2026-0227
3. https://security.paloaltonetworks.com/CVE-2026-0227