แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ Zero Day ของผลิตภัณฑ์ Palo Alto Networks (CVE-2024-3400)

วันที่แจ้งเตือน 17 เมษายน 2567

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่เป็นช่องโหว่ Zero Day ผลกระทบระดับร้ายแรงในผลิตภัณฑ์ Palo Alto Networks (CVE-2024-3400) ช่องโหว่ดังกล่าวเป็นช่องโหว่ “command injection” ในฟีเจอร์ GlobalProtect ของซอฟต์แวร์ PAN-OS ส่งผลให้ผู้ไม่หวังดีที่ไม่ได้รับการยืนยันตัวตน (unauthenticated) สามารถส่งคำสั่ง (arbitrary code) เข้าสู่ระบบได้ด้วยสิทธิสูง (root privileges)

โดยซอฟต์แวร์ ที่ได้รับผลกระทบ มีดังนี้

เวอร์ชัน	เวอร์ชันที่ได้รับผลกระทบ	เงื่อนไขการโจมตีช่องโหว่	ซอฟต์แวร์แก้ไขช่องโหว่
PAN-OS 10.2	< 10.2.6-h3, < 10.2.7-h8, < 10.2.8-h3, < 10.2.9-h1	PAN-OS เวอร์ชัน 10.2 /11.0 /11.1 ที่มีการเปิดการใช้งาน “GlobalProtect gateway” หรือ “GlobalProtect portal” (หรือเปิดใช้งานทั้ง 2 ฟีเจอร์) ทั้งนี้สามารถตรวจสอบการเปิดใช้งานฟีเจอร์ดังกล่าวได้ โดยไปที่ Network > GlobalProtect > Gateways หรือ Network > GlobalProtect > Portals	10.2.9-h1 (Released 4/14/24) 10.2.8-h3 (Released 4/15/24) 10.2.7-h8 (Released 4/15/24) 10.2.6-h3 (Released 4/16/24) 10.2.5-h6 (Released 4/16/24) 10.2.3-h13 (คาดว่า: 4/17/24) 10.2.1-h2 (คาดว่า: 4/17/24) 10.2.2-h5 (คาดว่า: 4/18/24) 10.2.0-h3 (คาดว่า: 4/18/24) 10.2.4-h16 (คาดว่า: 4/19/24)
PAN-OS 11.0	< 11.0.2-h4, < 11.0.3-h10, < 11.0.4-h1		11.0.4-h1 (Released 4/14/24) 11.0.3-h10 (Released 4/16/24) 11.0.2-h4 (Released 4/16/24) 11.0.1-h4 (คาดว่า: 4/17/24) 11.0.0-h3 (คาดว่า 4/18/24)
PAN-OS 11.1	< 11.1.0-h3, < 11.1.1-h1, < 11.1.2-h3		11.1.2-h3 (Released 4/14/24) 11.1.1-h1 (Released 4/16/24) 11.1.0-h3 (Released 4/16/24)

สำหรับผู้ใช้งานและผู้ดูแลที่ใช้บริการ Threat Prevention subscription สามารถปิดกั้นช่องโหว่ดังกล่าวโดยสามารถเปิดการป้องกัน Threat ID 95187 และ 95189 (ซึ่งจะปรากฏอยู่ใน “Applications and Threats content” เวอร์ชัน 8835-8689 เป็นต้นไป)

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 13 เม.ย. 2567
2) https://security.paloaltonetworks.com/CVE-2024-3400