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

แจ้งเตือนช่องโหว่ร้ายแรงของผลิตภัณฑ์ Fortinet SSL VPN (CVE-2024-21762)

วันที่แจ้งเตือน 12 กุมภาพันธ์ 2567

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Fortinet SSL VPN ที่อาจส่งผลให้ผู้ไม่หวังดีจากระยะไกลสามารถส่งคำสั่งที่ไม่ได้รับอนุญาต (arbitrary code) เข้าสู่ระบบได้ โดยไม่ต้องผ่านการยืนยันตัวตน

ทั้งนี้ Fortinet ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด ดังนี้

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

สำหรับผู้ใช้งานที่ไม่สามารถติดตั้งซอฟต์แวร์เป็นเวอร์ชันตามคำแนะนำได้ทันที ทาง Fortinet แนะนำวิธีแก้ปัญหาเบื้องต้น (workaround) ด้วยการปดการใช้งาน SSL VPN เพื่อเป็นการปองกันภัยคุกคามที่เกิดจากช่องโหว่ดังกล่าวเป็นการชั่วคราว

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 11 ก.พ. 2567
2) https://www.fortiguard.com/psirt/FG-IR-24-015
3) https://nvd.nist.gov/vuln/detail/CVE-2024-21762