แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ FortiSwitch (CVE-2024-48887)

วันที่แจ้งเตือน 24 เมษายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ FortiSwitch ที่เปิดใช้งาน web-based GUI โดยอาจส่งผลให้ผู้ไม่หวังดีจากระยะไกล สามารถเปลี่ยนรหัสผ่านผู้ดูแลระบบได้ผ่านคำขอ HTTP ที่ถูกออกแบบมาเป็นพิเศษ (crafted HTTP request) เพื่อหลีกเลี่ยงการยืนยันตัวตน และอาจมีดำเนินการเปลี่ยนแปลงรหัสผ่านของผู้ดูแลระบบ และเปลี่ยนแปลงการตั้งค่าระบบ รวมถึงขยายการโจมตีไปยังระบบหรืออุปกรณ์อื่น ๆ ภายในเครือข่ายได้ ทั้งนี้ Fortinet ได้ออกคำแนะนำให้ผู้ใช้งานพิจารณาอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด ดังตาราง

Version	Affected	Solution
FortiSwitch 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiSwitch 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiSwitch 7.2	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiSwitch 7.0	7.0.0 through 7.0.10	Upgrade to 7.0.11 or above
FortiSwitch 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above

สำหรับผู้ใช้งานที่ไม่สามารถติดตั้งซอฟต์แวร์เป็นเวอร์ชันตามคำแนะนำได้ทันที ทาง Fortinet แนะนำวิธีแก้ปัญหาเบื้องต้น (workaround) ดังนี้

- ปิดการเข้าถึงอินเทอร์เฟซการจัดการผ่าน web-based GUI (HTTP/HTTPS)
- เปิดใช้งานระบบยืนยันตัวตนแบบหลายปัจจัย (MFA) หากระบบรองรับ
- ตรวจสอบบันทึก (Logs) สำหรับกิจกรรมต้องสงสัย เช่น การเปลี่ยนรหัสผ่านหรือการเข้าถึง GUI เป็นต้น
- เฝ้าระวังการรับส่งข้อมูล HTTP ที่ผิดปกติซึ่งมุ่งเป้าไปยังอินเทอร์เฟซของ FortiSwitch
- จำกัดการเข้าถึงระบบจากเฉพาะเครื่องหรือเครือข่ายที่เชื่อถือได้

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 23 เม.ย. 2568
2) https://fortiguard.fortinet.com/psirt/FG-IR-24-435
3) https://nvd.nist.gov/vuln/detail/CVE-2024-48887