แจ้งเตือน : ช่องโหว่

Alert

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

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณีพบอุปกรณ Fortinet กวา 16,000 เครื่อง ถูกฝง Symlink Backdoor

วันที่แจ้งเตือน 24 เมษายน 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร โดย Shadowserver Foundation องค์กรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ไม่แสวงหากำไร พบวาอุปกรณ Fortinet อยางน้อย 16,000 เครื่องทั่วโลก ถูกฝง Symlink Backdoor โดยกลุมผูไม่หวังดีอาศัยชองโหวเดิม (CVE-2022-42475, CVE-2023-27997 และ CVE-2024-21762 เพื่อเขาถึงอุปกรณ์ Fortinet และ สราง Symlink* ที่เชื่อมโยงระหวางไฟลระบบของผูใชกับไฟลระบบ (root filesystem) ในโฟลเดอรของ SSL-VPN ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงไฟล์สำคัญ เชน /etc/passwd และ /config เป็นต้น เพื่ออ่านค่ารหัสผ่านและค่า config ของระบบได้โดยไมตองยกระดับสิทธิ

ทั้งนี้ Fortinet มีการส่งอีเมลแจ้งเตือนลูกค้าที่ใช้งานเป็นการส่วนตัว กรณีที่ตรวจพบว่าอุปกรณ์ของลูกค้าอาจได้รับผลกระทบจากการถูกฝง Symlink Backdoor ดังกล่าว

Fortinet แนะนำให้ผู้ดูแลระบบ พิจารณาดำเนินการ ดังนี้

- อัปเกรด FortiOS เปนเวอรชันลาสุดที่มีการปดชองโหว (FortiOS 7.6.2, 7.4.7, 7.2.11, 7.0.17, 6.4.16)
- รีเซ็ตรหัสผานของผูดูแลระบบทั้งหมด
- ตรวจสอบการตั้งคา Configuration ที่อาจถูกเปลี่ยนแปลง
- ปดการใชงาน SSL-VPN ชั่วคราวหากไมจำเปน
- ลบ symlink ที่นาสงสัย เชน rm/var/.sslvpn/lang/en เป็นต้น
- ตรวจสอบ Log เพื่อพิจารณาดำเนินการ กรณีพบการเขาถึงหรือพฤติกรรมที่นาสงสัย

*Symlink หรือ Symbolic Link คือ ไฟล์พิเศษชนิดหนึ่งในระบบปฏิบัติการ Unix/Linux ที่ทำหน้าที่เป็น “ทางลัด” หรือ “ตัวชี้” ไปยังไฟล์หรือโฟลเดอร์อื่น ซึ่งทำหน้าที่คล้ายกับ “Shortcut” บนระบบปฏิบัติการ Windows

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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 23 เม.ย. 2568
2) https://www.bleepingcomputer.com/news/security/over-16-000-fortinet-devices-compromised-with-symlink-backdoor/
3) https://community.fortinet.com/t5/FortiGate/Technical-Tip-Recommended-steps-to-execute-in-case-of-a/ta-p/230694