เอกสารการแจ้งเตือนกรณีพบอุปกรณ์ Fortinet กว่า 16,000 เครื่อง ถูกฝัง Symlink Backdoor

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณีพบอุปกรณ์ Fortinet กว่า 16,000 เครื่องถูกฝัง Symlink Backdoor

Shadowserver Foundation พบว่าอุปกรณ์ Fortinet FortiGate อย่างน้อย 16,000 เครื่องทั่วโลกถูกฝัง Symlink Backdoor โดยฝีมือของกลุ่มผู้โจมตีที่ใช้ช่องโหว่เดิม (CVE-2022-42475, CVE-2023-27997 และ CVE-2024-21762) เพื่อเข้าถึงอุปกรณ์ FortiGate และสร้าง Symlink ที่เชื่อมโยงระหว่างไฟล์ระบบของผู้ใช้กับไฟล์ระบบ (root filesystem) ในโฟลเดอร์ที่ใช้สำหรับไฟล์ภาษาของ SSL-VPN [1]

<u>จุดประสงค์ของการโจมตี</u>

ผู้โจมตีจะฝังไฟล์ Symlink Backdoor ภายใต้โฟลเดอร์ SSL VPN ใช้ Symlink เพื่อเข้าถึงไฟล์ระบบ เช่น /etc/passwd, /config โดยไม่ต้องยกระดับสิทธิ์ แม้จะมีการอัปเดตแพตช์เพื่อปิดช่องโหว่แล้ว แต่ Symlink ที่ถูกสร้างขึ้นยังคงอยู่ ทำให้ผู้โจมตีสามารถเข้าถึงไฟล์ภายในอุปกรณ์หรือไฟล์การตั้งค่าระบบได้ในระดับอ่าน (Read only)

<u>วิธีตรวจสอบไฟล์ Symlink Backdoor บนอุปกรณ์ FortiGate</u>

- เชื่อมต่อ FortiGate ผ่าน SSH หรือ Console ให้เข้าสู่ระบบ FortiGate ด้วยสิทธิ์ admin
- ตรวจสอบโฟลเดอร์ภาษาของ SSL VPN Symlink Backdoor มักถูกฝังไว้ใน Path: /var/.sslvpn/lang/ โดยใช้คำสั่ง: ls -l /var/.sslvpn/lang/ ไฟล์ปกติ ควรเป็น .txt หรือ .html และมีเจ้าของเป็น root

<u>สิ่งผิดปกติที่ควรระวัง</u>

- ไฟล์ที่แสดงว่าเป็น symlink (แสดงด้วย ->)
- ไฟล์ที่ลิงก์ไปยังตำแหน่งอื่นเช่น /etc/passwd, /config/, หรือ ../../.. (เพื่อหลบหลีกสิทธิ์)

ตัวอย่าง: lrwxrwxrwx 1 root root 14 Apr 3 14:20 en -> /etc/shadow แสดงว่าไฟล์ en เป็น symlink ที่ชี้ไปยัง /etc/shadow ถือว่าอันตราย

- ลบ symlink ที่น่าสงสัย เช่น rm/var/.sslvpn/lang/en
- ตรวจสอบด้วยไฟล์ Log สามารถดูการเข้าถึงหรือพฤติกรรมที่น่าสงสัยเพิ่มเติมได้โดย:
    - diagnose debug enable
    - diagnose debug application sslvpnd -1

และรอตรวจสอบ Log ที่แสดงว่า SSL VPN มีการโหลดไฟล์จาก Symlink หรือไม่

<u>คำแนะนำเพิ่มเติม</u>

- อัปเกรด FortiOS เป็นเวอร์ชั่นล่าสุดที่มีการปิดช่องโหว่ เช่น
    - FortiOS 7.0.17
    - FortiOS 7.2.11
    - FortiOS 7.4.7
    - FortiOS 6.4.16
- รีเซ็ตรหัสผ่านของผู้ดูแลระบบทั้งหมด
- ตรวจสอบการตั้งค่า ConFig ที่อาจถูกเปลี่ยน
- ปิดการใช้งาน SSL-VPN ชั่วคราวหากไม่จำเป็น [2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

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