วันที่ 29 มกราคม 2569

Fortinet ออกแพตช์แก้ไข CVE-2026-24858 หลังตรวจพบการโจมตี FortiOS SSO ที่เกิดขึ้นจริง

Fortinet ได้เริ่มปล่อยอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ร้ายแรงที่ส่งผลกระทบต่อ FortiOS ซึ่งขณะนี้กำลังถูกนำไปใช้โจมตีจริงในโลกไซเบอร์ ช่องโหว่นี้ถูกระบุด้วยรหัส CVE-2026-24858 และได้รับคะแนนความรุนแรงสูงถึง CVSS: 9.4 โดยเป็นปัญหาการข้ามขั้นตอนการยืนยันตัวตนที่เกี่ยวข้องกับระบบ Single Sign-On (SSO) ของ FortiOS

ช่องโหว่นี้ยังส่งผลกระทบต่อเนื่องไปถึง FortiManager และ FortiAnalyzer ด้วยเช่นกัน นอกจากนี้ Fortinet ระบุว่ายังคงอยู่ระหว่างการตรวจสอบว่าผลิตภัณฑ์อื่นๆ เช่น FortiWeb และ FortiSwitch Manager ได้รับผลกระทบจากช่องโหว่นี้ด้วยหรือไม่

เจาะลึกรายละเอียดทางเทคนิคของช่องโหว่

Fortinet ระบุไว้ในประกาศแจ้งเตือนเมื่อวันอังคารที่ผ่านมาว่า “ช่องโหว่ประเภทการข้ามการยืนยันตัวตนผ่านเส้นทางหรือช่องทางอื่น [CWE-288] ใน FortiOS, FortiManager และ FortiAnalyzer อาจเปิดโอกาสให้ผู้โจมตีที่มีบัญชี FortiCloud และมีอุปกรณ์ที่ลงทะเบียนไว้ สามารถล็อกอินเข้าไปยังอุปกรณ์อื่นที่ลงทะเบียนอยู่ภายใต้บัญชีคนละบัญชีได้ หากอุปกรณ์เหล่านั้นเปิดใช้งานการยืนยันตัวตนผ่าน FortiCloud SSO”

ทั้งนี้ ฟีเจอร์การล็อกอินด้วย FortiCloud SSO จะ ไม่ถูกเปิดใช้งานมาให้ตั้งแต่ค่าเริ่มต้นจากโรงงาน โดยจะถูกเปิดใช้งานเฉพาะในกรณีที่ผู้ดูแลระบบทำการลงทะเบียนอุปกรณ์กับ FortiCare ผ่านหน้า GUI ของอุปกรณ์เท่านั้น เว้นแต่ผู้ดูแลจะไปเปิดสวิตช์ “Allow administrative login using FortiCloud SSO” ด้วยตนเอง

เบื้องหลังแคมเปญการโจมตี: เส้นทางใหม่ของผู้ไม่หวังดี

ความเคลื่อนไหวครั้งนี้เกิดขึ้นเพียงไม่กี่วันหลังจาก Fortinet ยืนยันว่ามีกลุ่มผู้ไม่หวังดีที่ยังไม่ทราบตัวตน ใช้ “เส้นทางการโจมตีรูปแบบใหม่” เพื่อเข้าสู่ระบบ SSO ได้โดยไม่ต้องผ่านการยืนยันตัวตน การเข้าถึงดังกล่าวถูกนำไปใช้เพื่อ:

- สร้างบัญชีผู้ดูแลระบบใหม่เพื่อคงการควบคุมระบบไว้ (Persistence)

- เปลี่ยนการตั้งค่าเพื่อให้บัญชีเหล่านั้นสามารถเชื่อมต่อ VPN ได้
- ดึงข้อมูลการตั้งค่า (Configuration) ของไฟร์วอลล์ออกไปจากระบบ

Timeline การตอบสนองของ Fortinet

ในช่วงสัปดาห์ที่ผ่านมา Fortinet ได้ดำเนินมาตรการตอบโต้ดังนี้:

- 22 มกราคม 2026: ดำเนินการล็อกบัญชี FortiCloud ที่เป็นอันตรายจำนวน 2 บัญชี ได้แก่ “cloud-noc@mail.io” และ “cloud-init@mail.io”
- 26 มกราคม 2026: ปิดการใช้งาน FortiCloud SSO ในฝั่งของระบบ FortiCloud ทั้งหมด
- 27 มกราคม 2026: เปิดใช้งาน FortiCloud SSO อีกครั้ง พร้อมทั้ง ปิดกั้นไม่ให้อุปกรณ์ที่ยังใช้ซอฟต์แวร์เวอร์ชันที่มีช่องโหว่สามารถล็อกอินได้ ซึ่งหมายความว่าผู้ใช้งานจำเป็นต้องอัปเกรดซอฟต์แวร์เป็นเวอร์ชันล่าสุดก่อน จึงจะสามารถกลับมาใช้งานการยืนยันตัวตนผ่าน FortiCloud SSO ได้ตามปกติ

มาตรการรับมือเร่งด่วนสำหรับผู้ดูแลระบบ

Fortinet แนะนำอย่างเร่งด่วนว่า หากพบสัญญาณว่าระบบอาจถูกบุกรุก ควรถือว่าอุปกรณ์นั้นถูกเจาะแล้ว และให้ดำเนินการดังต่อไปนี้ทันที:

1. ตรวจสอบให้แน่ใจว่าอุปกรณ์ใช้เฟิร์มแวร์เวอร์ชันล่าสุด
2. กู้คืนการตั้งค่าจากไฟล์ที่มั่นใจว่าสะอาด หรือทำการตรวจสอบว่ามีการเปลี่ยนแปลงที่ไม่ได้รับอนุญาตหรือไม่
3. เปลี่ยนรหัสผ่านทั้งหมด รวมถึงบัญชี LDAP/AD ที่อาจเชื่อมต่อกับอุปกรณ์ FortiGate

การขยับตัวของ CISA

เหตุการณ์นี้ทำให้สำนักงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) เพิ่มรหัส CVE-2026-24858 เข้าไปในรายการ Known Exploited Vulnerabilities (KEV) ทันที และกำหนดให้หน่วยงานของรัฐบาลกลางสหรัฐฯ (FCEB) ต้องดำเนินการแก้ไขปัญหานี้ให้แล้วเสร็จภายในวันที่ 30 มกราคม 2026

ข้อมูลอ้างอิง

Jan 28, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/fortinet-patches-cve-2026-24858-after.html