วันที่ 26 มกราคม 2569

Fortinet ยืนยันพบการโจมตีข้ามระบบยืนยันตัวตน FortiCloud SSO บนไฟร์วอลล์ FortiGate ที่อัปเดตแพตช์แล้ว

Fortinet ได้ออกมายืนยันอย่างเป็นทางการว่า บริษัทกำลังเร่งดำเนินการแก้ไขช่องโหว่การข้ามระบบยืนยันตัวตนของ FortiCloud SSO อย่างสมบูรณ์ หลังจากที่มีรายงานตรวจพบการโจมตีรูปแบบใหม่ที่เกิดขึ้นกับไฟร์วอลล์ ซึ่งแม้ว่าจะได้รับการอัปเดตแพตช์ล่าสุดเรียบร้อยแล้วก็ตาม

Carl Windsor ประธานเจ้าหน้าที่ด้านความปลอดภัยสารสนเทศ (CISO) ของ Fortinet ได้ระบุไว้ในโพสต์เมื่อวันพฤหัสบดีที่ผ่านมาว่า “ภายในช่วง 24 ชั่วโมงที่ผ่านมา เราพบหลายกรณีที่การโจมตีเกิดขึ้นกับอุปกรณ์ที่ได้อัปเกรดเป็นเวอร์ชันล่าสุดในขณะนั้นแล้ว ซึ่งบ่งชี้ว่าเป็นเส้นทางการโจมตีรูปแบบใหม่”

วิเคราะห์การโจมตี: การเลี่ยงผ่านแพตช์ (Patch Bypass)

การโจมตีที่ตรวจพบในครั้งนี้ถือเป็นการเลี่ยงแพตช์ (Bypass) ที่ Fortinet เคยออกมาก่อนหน้านี้เพื่อแก้ไขช่องโหว่หมายเลข CVE-2025-59718 และ CVE-2025-59719 ซึ่งเป็นช่องโหว่ที่เปิดโอกาสให้ผู้โจมตีสามารถข้ามขั้นตอนการยืนยันตัวตนของระบบ SSO ได้โดยไม่ต้องผ่านการยืนยันตัวตนจริง หากมีการเปิดใช้งานฟีเจอร์ FortiCloud SSO บนอุปกรณ์ที่ได้รับผลกระทบ โดยช่องโหว่เหล่านี้ทาง Fortinet ได้ออกแพตช์แก้ไขไปแล้วตั้งแต่เดือนที่ผ่านมา

อย่างไรก็ตาม ในช่วงต้นสัปดาห์นี้ กลับมีรายงานการโจมตีระลอกใหม่ ซึ่งพบการล็อกอินผ่าน SSO ที่เป็นอันตรายเข้าสู่บัญชีผู้ดูแลระบบ (admin) บนอุปกรณ์ FortiGate ที่ได้ติดตั้งแพตช์ป้องกันช่องโหว่ทั้งสองรายการดังกล่าวเรียบร้อยแล้ว ลักษณะของเหตุการณ์ในครั้งนี้มีความคล้ายคลึงกับเหตุการณ์ที่เคยเกิดขึ้นในเดือนธันวาคมที่ผ่านมา ซึ่งเกิดขึ้นไม่นานหลังจากที่มีการเปิดเผยช่องโหว่ CVE-2025-59718 และ CVE-2025-59719 เป็นครั้งแรก

รูปแบบและพฤติกรรมการโจมตีที่ตรวจพบ

จากการตรวจสอบพบว่ารูปแบบการโจมตีในระลอกนี้ประกอบด้วย:

- การสร้างบัญชีผู้ใช้ทั่วไป: เพื่อใช้เป็นช่องทางในการฝังตัว (Persistence) อยู่ภายในระบบ
- การปรับแต่งค่าคอนฟิก: เพื่อให้บัญชีที่สร้างขึ้นใหม่เหล่านั้นสามารถเข้าใช้งาน VPN ได้
- การดึงข้อมูลสำคัญ: มีการดึงข้อมูลการตั้งค่า (Configuration) ของไฟร์วอลล์ออกไปยังหมายเลข IP ภายนอกที่ผู้โจมตีควบคุม
- ชื่อบัญชีที่ใช้โจมตี: พบว่าผู้โจมตีมีการล็อกอินด้วยชื่อบัญชี เช่น “cloud-noc@mail.io” และ “cloud-init@mail.io”

แนวทางลดความเสี่ยงเร่งด่วนจาก Fortinet

ในส่วนของแนวทางปฏิบัติเพื่อลดความเสี่ยงในระหว่างที่รอการแก้ไขอย่างสมบูรณ์ Fortinet แนะนำให้ผู้ดูแลระบบดำเนินการดังต่อไปนี้:

1. จำกัดการเข้าถึง: จำกัดสิทธิ์การเข้าถึงระบบบริหารจัดการของผู้ดูแลระบบ (Management Access) สำหรับอุปกรณ์เครือข่ายที่เชื่อมต่อกับอินเทอร์เน็ต โดยการกำหนด local-in policy ให้เข้มงวด
2. ปิดการใช้งานฟีเจอร์เสี่ยง: ปิดการใช้งาน FortiCloud SSO login โดยการปิดค่าคอนฟิกที่ชื่อว่า “admin-forticloud-sso-login”

คำเตือนเพิ่มเติมจาก Fortinet: ทางบริษัทระบุเพิ่มเติมว่า “แม้ในขณะนี้จะพบการโจมตีผ่าน FortiCloud SSO เท่านั้น แต่ปัญหานี้สามารถเกิดขึ้นได้กับการใช้งาน SAML SSO ทุกประเภท” ดังนั้นผู้ดูแลระบบที่ใช้งาน SAML SSO ควรเพิ่มความระมัดระวังและตรวจสอบระบบอย่างใกล้ชิด

ข้อมูลอ้างอิง

Jan 23, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/fortinet-confirms-active-forticloud-sso.html