วันที่ 23 มกราคม 2569

การโจมตี FortiGate ผ่านช่องโหว่ FortiCloud SSO เพื่อแก้ไขค่าคอนฟิกไฟร์วอลล์โดยไม่ได้รับอนุญาต

บริษัทด้านความปลอดภัยไซเบอร์ Arctic Wolf ได้ออกมาประกาศเตือนถึงการตรวจพบ “กลุ่มกิจกรรมอันตรายแบบอัตโนมัติรูปแบบใหม่” ซึ่งมีความเกี่ยวข้องกับการเปลี่ยนแปลงค่าคอนฟิกของไฟร์วอลล์ Fortinet FortiGate โดยไม่ได้รับอนุญาต ซึ่งกำลังส่งผลกระทบต่อผู้ใช้งานในวงกว้าง

ที่มาและลักษณะการโจมตีทางเทคนิค

Arctic Wolf ระบุว่า กิจกรรมดังกล่าวได้เริ่มต้นขึ้นเมื่อวันที่ 15 มกราคม 2026 โดยมีลักษณะพฤติกรรมคล้ายคลึงกับแคมเปญที่ตรวจพบในช่วงเดือนธันวาคม 2025 ซึ่งในขณะนั้นมีการพบการล็อกอินผ่านระบบ SSO บนอุปกรณ์ FortiGate อย่างผิดปกติ โดยเป็นการเข้าสู่ระบบด้วยบัญชีผู้ดูแล (admin) จากผู้ให้บริการโฮสติ้งหลายแห่ง ผ่านการโจมตีช่องโหว่รหัส CVE-2025-59718 และ CVE-2025-59719

ช่องโหว่ทั้งสองรายการนี้มีความร้ายแรงเนื่องจากเปิดโอกาสให้ผู้ไม่หวังดีสามารถข้ามขั้นตอนการยืนยันตัวตน (Authentication Bypass) ของระบบ SSO ได้โดยไม่ต้องผ่านการยืนยันตัวตนจริง เพียงแค่สร้างข้อความ SAML (Security Assertion Markup Language) ขึ้นมาเอง ในกรณีที่อุปกรณ์มีการเปิดใช้งานฟีเจอร์ FortiCloud single sign-on (SSO) อยู่ ซึ่งช่องโหว่ดังกล่าวส่งผลกระทบครอบคลุมทั้ง FortiOS, FortiWeb, FortiProxy และ FortiSwitchManager

พฤติกรรมการโจมตี: ยึดครองระบบด้วยความเร็วสูง

จากการวิเคราะห์ของ Arctic Wolf กิจกรรมในรอบนี้มีรูปแบบที่ชัดเจน ประกอบด้วยการสร้างบัญชีทั่วไปเพื่อใช้เป็นจุดยึดเกาะในระบบ (Persistence), การปรับค่าคอนฟิกเพื่อเปิดสิทธิ์ VPN ให้กับบัญชีเหล่านั้น รวมถึงการดึงไฟล์ค่าคอนฟิก (Config File) ของไฟร์วอลล์ออกไปจากระบบ

รายละเอียดการบุกรุกที่ตรวจพบ: ผู้โจมตีทำการล็อกอินผ่าน SSO ด้วยบัญชีที่เป็นอันตรายชื่อ “cloud-init@mail.io” โดยใช้ IP Address ที่แตกต่างกัน 4 รายการ จากนั้นจึงดำเนินการส่งออกไฟล์ค่าคอนฟิกของไฟร์วอลล์ผ่านหน้าเว็บบริหารจัดการ (GUI) ไปยัง IP Address เดิมของผู้โจมตี โดยรายการ IP ที่ตรวจพบมีดังนี้:

- 104.28.244[.]115
- 104.28.212[.]114
- 217.119.139[.]50
- 37.1.209[.]19

นอกจากนี้ ผู้โจมตียังได้สร้างบัญชีผู้ดูแลระบบสำรองเพิ่มเติมเพื่อคงการเข้าถึงระบบไว้ในระยะยาว ได้แก่ชื่อบัญชี: “secadmin,” “itadmin,” “support,” “backup,” “remoteadmin” และ “audit”

ที่น่าตกใจคือ Arctic Wolf ระบุว่าเหตุการณ์ทั้งหมดนี้เกิดขึ้นภายในเวลาเพียงไม่กี่วินาทีต่อเนื่องกัน ซึ่งเป็นข้อบ่งชี้ที่ชัดเจนว่าเป็นกิจกรรมที่ทำโดยระบบอัตโนมัติ (Automated) ไม่ใช่การกระทำด้วยมือของมนุษย์แต่อย่างใด

ข้อกังวล: แพตช์ล่าสุดอาจยังไม่เพียงพอ?

การเปิดเผยข้อมูลครั้งนี้สอดคล้องกับโพสต์บนเว็บไซต์ Reddit ซึ่งมีผู้ใช้งานหลายรายรายงานว่าพบการล็อกอินผ่าน SSO ที่เป็นอันตรายเช่นกัน แม้ว่าอุปกรณ์ FortiOS จะได้รับการอัปเดตแพตช์เป็นเวอร์ชันล่าสุดแล้วก็ตาม โดยมีผู้ใช้รายหนึ่งให้ข้อมูลที่น่าสนใจว่า “ทีมพัฒนา Fortinet ยืนยันแล้วว่าช่องโหว่นี้ยังคงอยู่ หรือยังไม่ได้รับการแก้ไขในเวอร์ชัน 7.4.10”

ในขณะนี้ *The Hacker News* ได้ดำเนินการติดต่อ Fortinet เพื่อขอความคิดเห็นเพิ่มเติมเกี่ยวกับประเด็นดังกล่าว และจะรีบอัปเดตข้อมูลให้ทราบหากมีความคืบหน้าเพิ่มเติม

มาตรการป้องกันเบื้องต้น

ในระหว่างที่รอการตรวจสอบและแพตช์แก้ไขอย่างเป็นทางการ ผู้ดูแลระบบได้รับคำแนะนำให้ดำเนินการดังนี้เพื่อลดความเสี่ยง:

1. ปิดการตั้งค่า: ปิดฟีเจอร์ “admin-forticloud-sso-login” ทันทีเพื่อป้องกันการข้ามผ่านการยืนยันตัวตน
2. ตรวจสอบบัญชี: ตรวจสอบรายชื่อผู้ดูแลระบบว่ามีบัญชีแปลกปลอมตามชื่อที่ระบุข้างต้นหรือไม่
3. ตรวจสอบ Log: เฝ้าระวังการล็อกอินที่มาจาก IP Address ต้องสงสัยและกิจกรรมการ Export ไฟล์คอนฟิก

ข้อมูลอ้างอิง

Jan 22, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/automated-fortigate-attacks-exploit.html