วันที่ 26 ธันวาคม 2568

Fortinet เตือน พบการโจมตีจริง ใช้ช่องโหว่ FortiOS SSL VPN หลบเลี่ยง 2FA

Fortinet ได้มีการเปิดเผยเมื่อวันพุธที่ผ่านมาว่าได้ตรวจพบการใช้ช่องโหว่ FortiOS โจมตีจริงเมื่อไม่นานมานี้ โดยช่องโหว่ดังกล่าวคือ CVE-2020-12812 (คะแนนความรุนแรง CVSS: 5.2) เป็นช่องโหว่ด้านการยืนยันตัวตนที่ไม่ถูกต้องใน SSL VPN ของ FortiOS ซึ่งอาจทำให้ผู้ใช้สามารถล็อกอินได้สำเร็จโดยไม่ต้องยืนยันตัวตนขั้นที่สอง (2FA) หากมีการเปลี่ยนรูปแบบตัวพิมพ์เล็ก–ใหญ่ของชื่อผู้ใช้

Fortinet เคยอธิบายไว้ตั้งแต่เดือนกรกฎาคม 2020 ว่า “ปัญหานี้จะเกิดขึ้นเมื่อเปิดใช้การยืนยันตัวตนแบบสองขั้นตอน (2FA) ในการตั้งค่า ‘user local’ และกำหนดให้ประเภทการยืนยันตัวตนของผู้ใช้นั้นอ้างอิงไปยังระบบยืนยันตัวตนภายนอก เช่น LDAP สาเหตุเกิดจากการตรวจสอบชื่อผู้ใช้ที่คำนึงถึงตัวพิมพ์เล็ก–ใหญ่ไม่สอดคล้องกัน ระหว่างการยืนยันตัวตนแบบ local และแบบ remote”

ต่อมาพบว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริงโดยกลุ่มผู้ไม่หวังดีหลายกลุ่ม และรัฐบาลสหรัฐฯ ก็ได้ระบุให้ช่องโหว่นี้เป็นหนึ่งในช่องโหว่ที่ถูกนำมาใช้เป็นอาวุธในการโจมตีอุปกรณ์เครือข่ายที่อยู่ขอบระบบ (perimeter devices) ตั้งแต่ปี 2021

ในคำแนะนำฉบับใหม่ที่ออกเมื่อวันที่ 24 ธันวาคม 2025 Fortinet ระบุว่า การโจมตีให้ประสบความสำเร็จด้วย CVE-2020-12812 จำเป็นต้องมีการตั้งค่าดังต่อไปนี้พร้อมกัน

- มีการสร้างผู้ใช้แบบ local บน FortiGate พร้อมเปิดใช้ 2FA และอ้างอิงกลับไปยัง LDAP
- ผู้ใช้กลุ่มเดียวกันต้องเป็นสมาชิกของกลุ่มบนเซิร์ฟเวอร์ LDAP
- ต้องมีอย่างน้อยหนึ่งกลุ่มจาก LDAP ที่ผู้ใช้ 2FA เป็นสมาชิก ถูกนำมาตั้งค่าไว้บน FortiGate และกลุ่มนั้นถูกใช้งานในนโยบายการยืนยันตัวตน เช่น สำหรับผู้ดูแลระบบ, SSL VPN หรือ IPSEC VPN

หากเงื่อนไขเหล่านี้ครบถ้วน ช่องโหว่จะทำให้ผู้ใช้ LDAP ที่ตั้งค่า 2FA ไว้ สามารถข้ามขั้นตอนความปลอดภัยนี้ไปได้ และไปยืนยันตัวตนกับ LDAP โดยตรง ซึ่งเกิดจากการที่ FortiGate ตรวจสอบชื่อผู้ใช้แบบแยกตัวพิมพ์เล็ก–ใหญ่ ในขณะที่ระบบ LDAP ไม่แยก

Fortinet อธิบายเพิ่มเติมว่า “หากผู้ใช้ล็อกอินด้วยชื่อ ‘Jsmith’, ‘jSmith’, ‘JSmith’, ‘jsmiTh’ หรือรูปแบบใดก็ตามที่ไม่ตรงกับ ‘jsmith’ แบบตัวอักษรตรงกันทุกตัว FortiGate จะไม่จับคู่การล็อกอินกับผู้ใช้ local จากนั้น FortiGate จะพิจารณาวิธีการยืนยันตัวตนอื่นๆ ที่ตั้งค่าไว้ และจะไปตรวจสอบนโยบายการยืนยันตัวตนของไฟร์วอลล์รายการอื่น เมื่อไม่พบ jsmith ใน local user แล้ว FortiGate จะไปพบกลุ่มรองที่ตั้งค่าไว้ เช่น ‘Auth-Group’ และเชื่อมต่อไปยัง LDAP Server ซึ่งหากชื่อผู้ใช้และรหัสผ่านถูกต้อง การยืนยันตัวตนจะสำเร็จทันที โดยไม่สนใจการตั้งค่าใดๆ ใน local user policy ไม่ว่าจะเป็น 2FA หรือการปิดบัญชีผู้ใช้ก็ตาม”

ผลลัพธ์คือ ช่องโหว่นี้สามารถใช้ล็อกอินในระดับผู้ดูแลระบบหรือผู้ใช้ VPN ได้โดยไม่ต้องผ่าน 2FA

แนวทางแก้ไขและข้อแนะนำจาก Fortinet

Fortinet ได้แก้ไขพฤติกรรมดังกล่าวไปแล้วตั้งแต่เดือนกรกฎาคม 2020 โดยออก FortiOS เวอร์ชัน 6.0.10, 6.2.4 และ 6.4.1 องค์กรที่ยังไม่ได้อัปเดตเป็นเวอร์ชันเหล่านี้ สามารถใช้คำสั่งด้านล่างกับบัญชีผู้ใช้ local ทั้งหมด เพื่อป้องกันการหลบเลี่ยงการยืนยันตัวตน

- set username-case-sensitivity disable

สำหรับลูกค้าที่ใช้ FortiOS เวอร์ชัน 6.0.13, 6.2.10, 6.4.7, 7.0.1 หรือใหม่กว่า Fortinet แนะนำให้ใช้คำสั่งนี้

- set username-sensitivity disable

Fortinet ระบุว่า “เมื่อปิดการแยกตัวพิมพ์เล็ก–ใหญ่ของชื่อผู้ใช้ FortiGate จะมองว่า jsmith, JSmith, JSMITH และรูปแบบอื่นๆ ทั้งหมดเป็นผู้ใช้คนเดียวกัน ซึ่งจะช่วยป้องกันไม่ให้ระบบไปใช้การยืนยันตัวตนผ่านกลุ่ม LDAP ที่ตั้งค่าไม่ถูกต้อง”

นอกจากนี้ ยังควรพิจารณาลบกลุ่ม LDAP รองออก หากไม่ได้มีความจำเป็น เพราะจะช่วยตัดช่องทางการโจมตีนี้ออกทั้งหมด โดยหากชื่อผู้ใช้ไม่ตรงกับบัญชี local ระบบจะปฏิเสธการยืนยันตัวตนทันที

อย่างไรก็ตาม คำแนะนำฉบับใหม่นี้ไม่ได้ให้รายละเอียดเกี่ยวกับลักษณะของการโจมตีที่เกิดขึ้น ว่ามีรูปแบบใดบ้าง หรือมีเหตุการณ์ใดประสบความสำเร็จจริงหรือไม่

Fortinet ยังแนะนำให้ลูกค้าที่ได้รับผลกระทบ ติดต่อทีมสนับสนุนของบริษัท และรีเซ็ตรหัสผ่านทั้งหมด หากพบหลักฐานว่ามีการล็อกอินของผู้ดูแลระบบหรือผู้ใช้ VPN โดยไม่ผ่านการยืนยันตัวตนแบบ 2FA

ข้อมูลอ้างอิง

Dec 26, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/12/fortinet-warns-of-active-exploitation.html