วันที่ 11 กุมภาพันธ์ 2569

Fortinet ออกแพตช์แก้ไขช่องโหว่ร้ายแรงแบบ SQL Injection ที่เปิดทางให้รันโค้ดได้โดยไม่ต้องยืนยันตัวตน

Fortinet ได้ออกอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ร้ายแรงที่ส่งผลกระทบต่อ FortiClientEMS ซึ่งอาจทำให้ผู้ไม่หวังดีสามารถรันโค้ดใดๆ ก็ได้บนระบบที่ได้รับผลกระทบ ช่องโหว่นี้ถูกติดตามด้วยรหัส CVE-2026-21643 และมีคะแนนความรุนแรง CVSS อยู่ที่ 9.1 จากคะแนนเต็ม 10.0 ช่องโหว่ประเภท SQL Injection [CWE-89] ซึ่งเกิดจากการจัดการคำสั่ง SQL ที่ไม่เหมาะสมใน FortiClientEMS อาจเปิดโอกาสให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตน และสามารถรันโค้ดหรือคำสั่งที่ไม่ได้รับอนุญาต ผ่านคำขอ HTTP ที่ถูกสร้างขึ้นมาเป็นพิเศษ Fortinet ระบุในประกาศแจ้งเตือน

ช่องโหว่นี้ส่งผลกระทบต่อเวอร์ชันดังต่อไปนี้

- FortiClientEMS 7.2 (ไม่ได้รับผลกระทบ)
- FortiClientEMS 7.4.4 (ควรอัปเกรดเป็นเวอร์ชัน 7.4.5 ขึ้นไป)
- FortiClientEMS 8.0 (ไม่ได้รับผลกระทบ)

Gwendal Guégniaud จากทีมความปลอดภัยผลิตภัณฑ์ของ Fortinet ได้รับเครดิตในการค้นพบและรายงานช่องโหว่นี้ แม้ว่า Fortinet จะไม่ได้ระบุว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริงแล้วหรือไม่ แต่ผู้ใช้งานควรรีบดำเนินการอัปเดตเพื่อปิดความเสี่ยงโดยเร็วที่สุด ความเคลื่อนไหวครั้งนี้เกิดขึ้นหลังจากที่บริษัทได้แก้ไขช่องโหว่ร้ายแรงอีกจุดหนึ่งใน FortiOS, FortiManager, FortiAnalyzer, FortiProxy และ FortiWeb (CVE-2026-24858, คะแนน CVSS: 9.4) ซึ่งอาจทำให้ผู้โจมตีที่มีบัญชี FortiCloud และมีอุปกรณ์ที่ลงทะเบียนไว้ สามารถเข้าสู่ระบบอุปกรณ์อื่นที่ลงทะเบียนภายใต้บัญชีคนละบัญชีได้ หากอุปกรณ์เหล่านั้นเปิดใช้งานการยืนยันตัวตนแบบ FortiCloud SSO ต่อมา Fortinet ยอมรับว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริง โดยผู้ไม่หวังดีได้สร้างบัญชีผู้ดูแลระบบภายในเครื่องเพื่อฝังตัวอยู่ในระบบ ทำการปรับเปลี่ยนค่าการตั้งค่าเพื่อเปิดสิทธิ์การเชื่อมต่อ VPN ให้กับบัญชีดังกล่าว และดึงข้อมูลการตั้งค่าของไฟร์วอลล์ออกไปจากระบบ

ข้อมูลอ้างอิง

Feb 10, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/02/fortinet-patches-critical-sqli-flaw.html