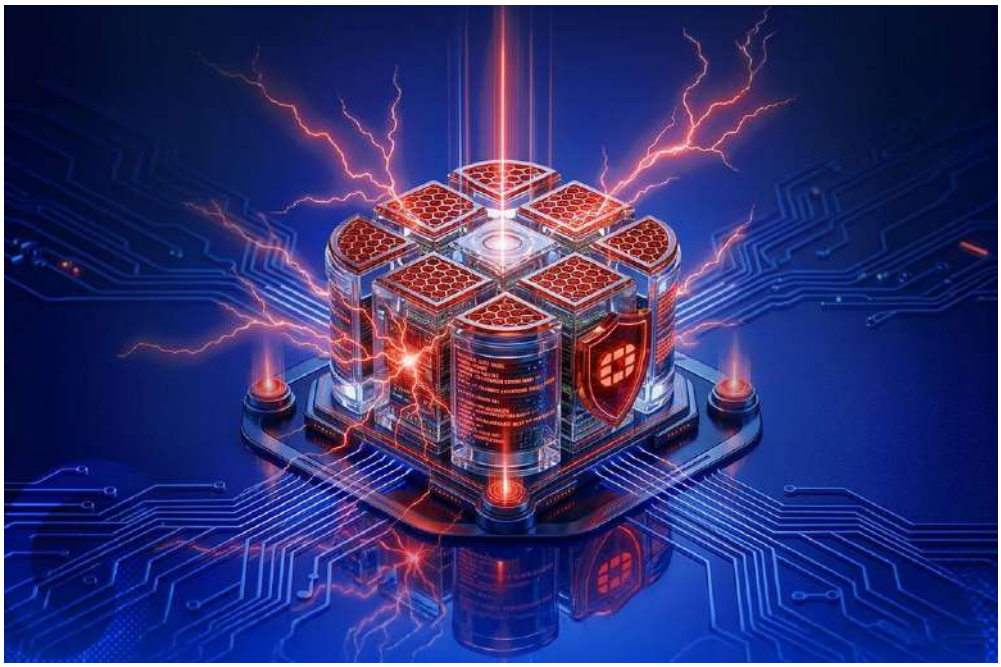
วันที่ 7 เมษายน 2569

Fortinet ออกแพตช์แก้ช่องโหว่ CVE-2026-35616 ที่กำลังถูกโจมตีจริงใน FortiClient EMS



Fortinet ได้ออกแพตช์แบบเร่งด่วน (out-of-band) เพื่อแก้ไขช่องโหว่ด้านความปลอดภัยระดับร้ายแรงที่ส่งผลกระทบต่อ FortiClient EMS โดยบริษัทระบุว่าช่องโหว่นี้กำลังถูกนำไปใช้โจมตีจริงแล้วในขณะนี้ ช่องโหว่นี้ถูกติดตามในชื่อ CVE-2026-35616 (คะแนนความรุนแรง CVSS 9.1) และถูกอธิบายว่าเป็นช่องโหว่ที่สามารถ ข้ามการยืนยันตัวตนของ API ก่อนการล็อกอิน (pre-authentication API access bypass) และนำไปสู่การ ยกระดับสิทธิ์การเข้าถึงระบบ (privilege escalation)

เตือนภัยช่องโหว่ร้ายแรงใน FortiClient EMS

Fortinet ได้ออกคำแนะนำด้านความปลอดภัยเมื่อวันเสาร์ที่ผ่านมา เพื่อแจ้งเตือนเกี่ยวกับช่องโหว่ด้านการควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสมในระบบ FortiClient EMS ช่องโหว่นี้มีความอันตรายอย่างมาก เนื่องจากเปิดโอกาสให้ผู้โจมตีที่ยังไม่ได้ยืนยันตัวตน สามารถรันโค้ดหรือคำสั่งที่ไม่ได้รับอนุญาตได้ เพียงแค่ส่งคำขอที่ถูกสร้างขึ้นมาเป็นพิเศษ ปัจจุบันปัญหานี้ส่งผลกระทบโดยตรงต่อผู้ใช้งาน FortiClient EMS เวอร์ชัน 7.4.5 ถึง 7.4.6 โดยคาดว่าจะได้รับการแก้ไขอย่างสมบูรณ์ในเวอร์ชัน 7.4.7 ที่กำลังจะออกมา อย่างไรก็ตาม บริษัทได้ปล่อย hotfix เพื่อแก้ไขช่องโหว่นี้แล้ว

สำหรับผู้ที่ค้นพบและรายงานช่องโหว่นี้คือคุณ Simo Kohonen จาก Defused Cyber และคุณ Nguyen Duc Anh โดยทาง Defused Cyber ได้ระบุผ่านแพลตฟอร์ม X ว่าพบการโจมตีแบบ Zero-day ที่ใช้ช่องโหว่ CVE-2026-35616 มาตั้งแต่ช่วงต้นสัปดาห์ที่ผ่านมา ขณะเดียวกัน บริษัท watchTowr เปิดเผยว่า ระบบ honeypot ของตนเริ่มตรวจพบความพยายามโจมตีช่องโหว่นี้ครั้งแรกเมื่อวันที่ 31 มีนาคม 2026

อันตรายจากการเจาะระบบและช่องโหว่ที่ซ้อนทับ

หากผู้โจมตีสามารถใช้ช่องโหว่นี้ได้สำเร็จ จะสามารถข้ามผ่านระบบยืนยันตัวตนและการตรวจสอบสิทธิ์ของ API ทำให้สามารถรันโค้ดหรือคำสั่งอันตรายในระบบได้อย่างอิสระ ล่าสุดทาง Fortinet ระบุเพิ่มเติมว่า Fortinet ตรวจพบว่าช่องโหว่นี้กำลังถูกนำไปใช้โจมตีจริงแล้ว และขอแนะนำให้ผู้ที่ใช้งาน FortiClient EMS เวอร์ชัน 7.4.5 และ 7.4.6 ติดตั้ง hotfix โดยเร็วที่สุด

เหตุการณ์นี้เกิดขึ้นเพียงไม่กี่วันหลังจากที่มีช่องโหว่ร้ายแรงอีกตัวหนึ่งใน FortiClient EMS คือ CVE-2026-21643 (คะแนน CVSS 9.1) ซึ่งเพิ่งได้รับการแก้ไขไปไม่นาน และปัจจุบันก็พบว่ากำลังถูกโจมตีจริงเช่นกัน ขณะนี้ยังไม่ทราบแน่ชัดว่า ผู้โจมตีรายเดียวกันอยู่เบื้องหลังการใช้ช่องโหว่ทั้งสองตัวหรือไม่ และยังไม่ชัดเจนว่ามีการนำช่องโหว่ทั้งสองมาใช้ร่วมกันในการโจมตีด้วยความรุนแรงของช่องโหว่ดังกล่าว ผู้ใช้งานจึงควร อัปเดต FortiClient EMS เป็นเวอร์ชันล่าสุดโดยเร็วที่สุด

ประกาศสถานการณ์ฉุกเฉิน ไม่ควรรอถึงวันทำงาน

คุณ Benjamin Harris ซีอีโอและผู้ก่อตั้งของ watchTowr ให้สัมภาษณ์กับ The Hacker News ว่า ช่วงเวลาที่การโจมตีแบบ zero-day เพิ่มขึ้นอย่างรวดเร็วในช่วงเวลานี้ อาจไม่ใช่เรื่องบังเอิญ ผู้โจมตีพิสูจน์มาแล้วหลายครั้งว่า ช่วงวันหยุดยาวเป็นเวลาที่เหมาะที่สุดในการลงมือ เพราะทีมรักษาความปลอดภัยมักมีคนทำงานน้อย ซึ่งในช่วงเวลาระหว่างการถูกเจาะระบบจนถึงการตรวจพบก็อาจยืดออกจากไม่กี่ชั่วโมงเป็นหลายวันได้

ดังนั้น องค์กรที่ใช้ FortiClient EMS และเปิดให้เข้าถึงได้จากอินเทอร์เน็ต ควรมองว่านี่คือสถานการณ์ฉุกเฉินด้านความปลอดภัย ที่ไม่ควรรอจัดการในวันทำงานถัดไป แต่ต้องติดตั้ง Hotfix ทันที

สหรัฐฯ ขีดเส้นตาย บังคับอุดช่องโหว่ทันที

เมื่อวันที่ 6 เมษายน 2026 หน่วยงาน Cybersecurity and Infrastructure Security Agency (CISA) ของสหรัฐฯ ได้เพิ่มช่องโหว่ CVE-2026-35616 ลงในรายการ Known Exploited Vulnerabilities (KEV) และกำหนดให้หน่วยงานภาครัฐในกลุ่ม Federal Civilian Executive Branch (FCEB) ต้องดำเนินการติดตั้งแพตช์แก้ไขภายในวันที่ 9 เมษายน 2026

ข้อมูลอ้างอิง

Apr 5, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/fortinet-patches-actively-exploited-cve.html