วันที่ 22 สิงหาคม 2568

Cisco เตือนช่องโหว่ร้ายแรงระดับ CVSS 10.0 ใน FMC RADIUS ที่อาจถูกใช้โจมตีเพื่อรันโค้ดจากระยะไกล

Cisco ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ที่มีความรุนแรงสูงสุดในซอฟต์แวร์ Secure Firewall Management Center (FMC) ซึ่งอาจเปิดทางให้ผู้โจมตีสามารถรันโค้ดที่ต้องการบนระบบได้โดยสมบูรณ์

ช่องโหว่นี้ได้รับการกำหนดหมายเลขเป็น CVE-2025-20265 และได้คะแนน CVSS เต็ม 10.0 ซึ่งถือว่าร้ายแรงที่สุด โดยเกิดขึ้นในส่วนการทำงานของ RADIUS ที่มีข้อบกพร่อง ทำให้ผู้โจมตีซึ่งไม่ได้ยืนยันตัวตนสามารถส่งคำสั่งพิเศษแอบแฝงเข้ามาได้ และคำสั่งเหล่านั้นจะถูกประมวลผลโดยอุปกรณ์

รายละเอียดช่องโหว่และเงื่อนไขการโจมตี

Cisco ระบุว่าปัญหามีสาเหตุมาจากการตรวจสอบข้อมูลที่ผู้ใช้งานกรอกเข้ามาในขั้นตอนการยืนยันตัวตนไม่สมบูรณ์ เมื่อข้อมูลที่ถูกสร้างขึ้นมาเฉพาะเจาะจงถูกใส่ในช่องข้อมูลยืนยันตัวตนและถูกส่งไปยังเซิร์ฟเวอร์ RADIUS ที่ตั้งค่าไว้ ก็จะสามารถทำให้คำสั่งถูกประมวลผลได้

“หากการโจมตีสำเร็จ ผู้โจมตีสามารถรันคำสั่งในระดับสิทธิ์สูงได้” บริษัทกล่าวไว้ในคำแนะนำ “การจะโจมตีช่องโหว่นี้ได้ ซอฟต์แวร์ Cisco Secure FMC ต้องถูกตั้งค่าให้ใช้ RADIUS สำหรับการยืนยันตัวตนในการเข้าใช้งานผ่านหน้าเว็บ, การจัดการผ่าน SSH หรือทั้งสองอย่าง”

ช่องโหว่นี้ส่งผลกระทบต่อ Cisco Secure FMC Software เวอร์ชัน 7.0.7 และ 7.7.0 ที่เปิดใช้ RADIUS authentication โดยไม่มีวิธีแก้ปัญหาอื่นนอกจากต้องติดตั้งแพตช์ที่ Cisco ปล่อยออกมา ช่องโหว่นี้ถูกค้นพบโดย Brandon Sakai จาก Cisco ในระหว่างการทดสอบความปลอดภัยภายใน

รายการช่องโหว่ร้ายแรงอื่น ๆ ที่ได้รับการแก้ไข

นอกจาก CVE-2025-20265 แล้ว Cisco ยังได้แก้ไขช่องโหว่ความรุนแรงสูงอีกหลายรายการ ซึ่งส่วนใหญ่เกี่ยวข้องกับการโจมตีแบบ DoS (Denial of Service) และ RCE (Remote Code Execution):

- CVE-2025-20217 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco Secure Firewall Threat Defense Software Snort 3
- CVE-2025-20222 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco Secure Firewall ASA และ Secure Firewall Threat Defense สำหรับ Firepower 2100 Series เกี่ยวกับ IPv6 over IPsec
- CVE-2025-20224, CVE-2025-20225, CVE-2025-20239 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco IOS, IOS XE, ASA และ Secure Firewall Threat Defense เกี่ยวกับ IKEv2
- CVE-2025-20133, CVE-2025-20243 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense เกี่ยวกับ Remote Access SSL VPN
- CVE-2025-20134 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense เกี่ยวกับ SSL/TLS Certificate
- CVE-2025-20136 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense เกี่ยวกับ NAT DNS Inspection
- CVE-2025-20263 (CVSS 8.6): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense เกี่ยวกับ Web Services
- CVE-2025-20148 (CVSS 8.5): ช่องโหว่ HTML Injection ใน Cisco Secure Firewall Management Center
- CVE-2025-20251 (CVSS 8.5): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense เกี่ยวกับ VPN Web Server
- CVE-2025-20127 (CVSS 7.7): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense สำหรับ Firepower 3100 และ 4200 Series เกี่ยวกับ TLS 1.3 Cipher
- CVE-2025-20244 (CVSS 7.7): ช่องโหว่ DoS ใน Cisco ASA และ Secure Firewall Threat Defense เกี่ยวกับ Remote Access VPN Web Server

แม้ว่าจะยังไม่พบการโจมตีช่องโหว่เหล่านี้จริงในโลกภายนอก แต่เนื่องจากอุปกรณ์เครือข่ายมักตกเป็นเป้าหมายของผู้โจมตีอยู่บ่อยครั้ง ผู้ใช้งานจึงควรเร่งอัปเดตซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดโดยเร็วที่สุด

ข้อมูลอ้างอิง

Aug 15, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/cisco-warns-of-cvss-100-fmc-radius-flaw.html