วันที่ 4 กรกฎาคม 2568

ช่องโหว่สำคัญของ Cisco ใน Unified CM อนุญาตให้เข้าถึงรูทผ่านข้อมูลประจำตัว

Cisco ได้ออกอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ความรุนแรงสูงสุดในผลิตภัณฑ์ Unified Communications Manager (Unified CM) และ Unified Communications Manager Session Management Edition (Unified CM SME) ช่องโหว่นี้อาจเปิดทางให้แฮกเกอร์ล็อกอินเข้าอุปกรณ์ที่มีช่องโหวในฐานะผู้ใช้ root ทำให้สามารถเข้าถึงสิทธิ์สูงสุดได้

ช่องโหว่นี้ถูกติดตามในรหัส CVE-2025-20309 โดยมีคะแนนความรุนแรง CVSS อยู่ที่ 10.0 ซึ่งบ่งชี้ว่าเป็นภัยคุกคามระดับวิกฤต

"ช่องโหว่นี้เกิดจากการมีบัญชีผู้ใช้ root ที่ใช้รหัสผ่านตายตัว (static credentials) ซึ่งถูกสงวนไว้สำหรับการพัฒนา" Cisco ระบุในประกาศแจ้งเตือนที่เผยแพร่เมื่อวันพุธ "แฮกเกอร์สามารถใช้ช่องโหว่นี้โดยล็อกอินด้วยบัญชีดังกล่าวเข้าสู่ระบบที่ได้รับผลกระทบ หากการโจมตีสำเร็จ แฮกเกอร์จะสามารถล็อกอินเข้าสู่ระบบและรันคำสั่งใดๆ ได้ในสิทธิ์ของผู้ใช้ root"

รหัสผ่านตายตัวแบบนี้มักเกิดจากการทดสอบหรือการแก้ไขชั่วคราวระหว่างการพัฒนา แต่ไม่ควรหลุดมาอยู่ในระบบที่ใช้งานจริง โดยเฉพาะในเครื่องมืออย่าง Unified CM ที่ทำหน้าที่จัดการการโทรและการสื่อสารภายในองค์กร เพราะสิทธิ์ root จะเปิดช่องให้แฮกเกอร์เคลื่อนย้ายลึกเข้าไปในเครือข่าย แอบดักฟังการโทร หรือเปลี่ยนวิธีการล็อกอินของผู้ใช้ได้

Cisco กล่าวว่า ขณะนี้ยังไม่พบหลักฐานว่าช่องโหว่นี้ถูกใช้โจมตีจริง และช่องโหว่นี้ถูกค้นพบระหว่างการทดสอบความปลอดภัยภายใน

เวอร์ชันที่ได้รับผลกระทบและวิธีตรวจสอบ:

CVE-2025-20309 ส่งผลกระทบกับ Unified CM และ Unified CM SME เวอร์ชัน 15.0.1.13010-1 ถึง 15.0.1.13017-1 โดยไม่ขึ้นกับการตั้งค่าของอุปกรณ์

Cisco ยังได้เผยตัวชี้วัดการถูกโจมตี (Indicators of Compromise – IoCs) ที่เกี่ยวข้องกับช่องโหว่นี้ โดยหากการโจมตีสำเร็จจะมีบันทึกอยู่ในไฟล์ล็อก “/var/log/active/syslog/secure” สำหรับผู้ใช้ root ที่ได้รับสิทธิ์ root ซึ่งสามารถดึงไฟล์ล็อกนี้ได้จากคำสั่งใน CLI ดังนี้:

```
cucm1# file get activelog syslog/secure
```

เหตุการณ์นี้เกิดขึ้นเพียงไม่กี่วันหลังจากที่ Cisco เพิ่งแก้ไขช่องโหว่ความปลอดภัยสองรายการใน Identity Services Engine และ ISE Passive Identity Connector (CVE-2025-20281 และ CVE-2025-20282) ซึ่งอาจเปิดทางให้แฮกเกอร์ที่ไม่ได้รับการยืนยันตัวตนสามารถรันคำสั่งใดๆ ด้วยสิทธิ์ root ได้เช่นกัน

การพบช่องโหว่ที่มีรหัสผ่านตายตัวในผลิตภัณฑ์สำคัญอย่าง Cisco Unified CM ถือเป็นความเสี่ยงด้านความปลอดภัยที่ร้ายแรงอย่างยิ่ง ผู้ดูแลระบบจึงควรดำเนินการอัปเดตแพตช์โดยทันที เพื่อปิดช่องโหว่นี้และป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งอาจนำไปสู่การควบคุมโครงสร้างพื้นฐานด้านการสื่อสารทั้งหมดขององค์กรได้

ข้อมูลอ้างอิง

July 3, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/07/critical-cisco-vulnerability-in-unified.html