วันที่ 1 กรกฎาคม 2568

ช่องโหว่ RCE ที่สำคัญใน Cisco ISE และ ISE-PIC ทำให้ผู้โจมตีสามารถเข้าถึงสิทธิ์รูทได้

Cisco ได้ออกอัปเดตสำคัญเพื่อแก้ไขช่องโหว่ด้านความปลอดภัยระดับร้ายแรงสูงสุด 2 รายการในผลิตภัณฑ์ **Identity Services Engine (ISE)** และ **ISE Passive Identity Connector (ISE-PIC)** ช่องโหว่เหล่านี้อาจทำให้ผู้โจมตีที่ไม่ได้รับการยืนยันตัวตนสามารถรันคำสั่งใดๆ บนระบบปฏิบัติการในระดับ **root** ได้

ช่องโหว่เหล่านี้ได้รับหมายเลข **CVE-2025-20281** และ **CVE-2025-20282** โดยแต่ละช่องโหว่มีคะแนน **CVSS สูงสุดที่ 10.0** ซึ่งบ่งชี้ถึงความรุนแรงระดับวิกฤต

รายละเอียดช่องโหว่:

- CVE-2025-20281:
  - เป็นช่องโหว่ที่ทำให้สามารถ **รันโค้ดจากระยะไกลโดยไม่ต้องยืนยันตัวตน** (Remote Code Execution - RCE)
  - กระทบกับ **Cisco ISE และ ISE-PIC เวอร์ชัน 3.3 ขึ้นไป**
  - ผู้โจมตีที่ไม่ได้ยืนยันตัวตนสามารถรันโค้ดใดๆ บนระบบปฏิบัติการในระดับ root
- CVE-2025-20282:
  - เป็นช่องโหว่ที่ทำให้สามารถ **รันโค้ดจากระยะไกลโดยไม่ต้องยืนยันตัวตน** (Remote Code Execution - RCE)
  - กระทบกับ **Cisco ISE และ ISE-PIC เวอร์ชัน 3.4**
  - ผู้โจมตีที่ไม่ได้ยืนยันตัวตนสามารถอัปโหลดไฟล์ใดๆ ไปยังอุปกรณ์ที่ได้รับผลกระทบ และรันไฟล์เหล่านั้นบนระบบปฏิบัติการในระดับ root

Cisco ระบุว่า **CVE-2025-20281** เกิดจากการตรวจสอบค่าที่ผู้ใช้ส่งมาไม่เพียงพอ ซึ่งผู้โจมตีอาจใช้ประโยชน์จากช่องโหว่นี้ด้วยการส่งคำขอ API ที่ถูกสร้างขึ้นอย่างเจาะจง เพื่อให้ได้สิทธิ์ระดับสูงและสามารถรันคำสั่งได้

ในทางกลับกัน **CVE-2025-20282** เกิดจากการที่ไม่มีการตรวจสอบไฟล์อย่างเหมาะสม ซึ่งควรจะป้องกันไม่ให้ไฟล์ที่อัปโหลดถูกวางในไดเรกทอรีที่มีสิทธิพิเศษ

“หากการโจมตีสำเร็จ อาจทำให้ผู้โจมตีสามารถจัดเก็บไฟล์อันตรายบนระบบที่ได้รับผลกระทบ และรันโค้ดใดๆ หรือได้สิทธิ์ root บนระบบ” Cisco กล่าว

แนวทางการแก้ไขและการอัปเดตที่จำเป็น:

Cisco ผู้จำหน่ายอุปกรณ์เครือข่ายรายนี้ระบุว่า **ไม่มีวิธีแก้ไขปัญหาเฉพาะหน้า (workarounds) ที่สามารถใช้ป้องกันได้** ดังนั้น การอัปเดตแพตช์จึงเป็นสิ่งจำเป็นเร่งด่วน โดย Cisco ได้แก้ไขข้อบกพร่องเหล่านี้ในเวอร์ชันดังต่อไปนี้:

- **สำหรับ CVE-2025-20281:**
    - Cisco ISE หรือ ISE-PIC **3.3 Patch 6** (ise-apply-CSCwo99449_3.3.0.430_patch4-SPA.tar.gz)
    - **3.4 Patch 2** (ise-apply-CSCwo99449_3.4.0.608_patch1-SPA.tar.gz)
- **สำหรับ CVE-2025-20282:**
    - Cisco ISE หรือ ISE-PIC **3.4 Patch 2** (ise-apply-CSCwo99449_3.4.0.608_patch1-SPA.tar.gz)

Cisco ได้ให้เครดิต **Bobby Gould จาก Trend Micro Zero Day Initiative** และ **Kentaro Kawane จาก GMO Cybersecurity** ในการรายงาน CVE-2025-20281 โดย Kawane ซึ่งเคยรายงาน CVE-2025-20286 (คะแนน CVSS: 9.9) มาก่อนหน้านี้ ก็ได้รับการยกย่องในการรายงาน CVE-2025-20282 ด้วยเช่นกัน

แม้จะยังไม่มีหลักฐานว่าช่องโหว่เหล่านี้ถูกนำมาใช้โจมตีจริง แต่เป็นเรื่องสำคัญอย่างยิ่งที่ผู้ใช้งานควรรีบดำเนินการอัปเดตแพตช์เพื่อปกป้องตนเองจากความเสี่ยงที่อาจเกิดขึ้น

ช่องโหว่ระดับสูงสุดใน Cisco ISE และ ISE-PIC นี้เป็นภัยคุกคามที่ร้ายแรง เนื่องจากเปิดทางให้ผู้โจมตีสามารถควบคุมระบบได้ทั้งหมดโดยไม่ต้องยืนยันตัวตน ผู้ดูแลระบบควรดำเนินการอัปเดตแพตช์โดยทันทีเพื่อรักษาความปลอดภัยของโครงสร้างพื้นฐานขององค์กร

ข้อมูลอ้างอิง

Jun 26, 2025 By Ravie Lakshmanan

- https://thehackernews.com/2025/06/critical-rce-flaws-in-cisco-ise-and-ise.html