วันที่ 12 มกราคม 2569

Cisco ออกแพตช์อุดช่องโหว่ความปลอดภัยใน ISE หลังมีการเผยแพร่ PoC สู่สาธารณะ

Cisco ได้ดำเนินการออกอัปเดตเพื่อแก้ไขช่องโหว่ด้านความปลอดภัยระดับปานกลางใน Identity Services Engine (ISE) และ ISE Passive Identity Connector (ISE-PIC) หลังจากที่มีการเผยแพร่โค้ดตัวอย่างการโจมตี (Proof-of-Concept หรือ PoC) ออกสู่สาธารณะ ซึ่งช่องโหว่นี้ถูกติดตามด้วยรหัส CVE-2026-20029 (คะแนนความรุนแรง CVSS: 4.9) โดยเกิดขึ้นในฟีเจอร์ด้านไลเซนส์ (License) และอาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่มีสิทธิ์ผู้ดูแลระบบ สามารถเข้าถึงข้อมูลสำคัญได้

รายละเอียดทางเทคนิคของช่องโหว่ CVE-2026-20029

ทาง Cisco ระบุว่า “ช่องโหว่นี้เกิดจากการแปลผลไฟล์ XML ที่ไม่ถูกต้อง ซึ่งถูกประมวลผลผ่านหน้าเว็บสำหรับจัดการระบบของ Cisco ISE และ Cisco ISE-PIC ทำให้ผู้โจมตีสามารถใช้ช่องโหว่นี้ได้โดยการอัปโหลดไฟล์ที่ถูกสร้างขึ้นมาเข้าสู่ระบบ”

หากการโจมตีสำเร็จ ผู้โจมตีที่มีบัญชีผู้ดูแลระบบอยู่แล้ว จะสามารถอ่านไฟล์ใดก็ได้จากระบบปฏิบัติการภายใน ซึ่งตามปกติแล้วไฟล์เหล่านี้ไม่ควรเปิดให้เข้าถึงได้ แม้แต่ผู้ดูแลระบบเองก็ตาม โดยช่องโหว่นี้ถูกค้นพบและรายงานโดย Bobby Gould จากทีม Trend Micro Zero Day Initiative

เวอร์ชันที่ได้รับผลกระทบและการแก้ไข:

- Cisco ISE หรือ ISE-PIC รุ่นก่อนหน้า 3.2: แนะนำให้อัปเกรดไปยังรุ่นที่แก้ไขแล้ว
- Cisco ISE หรือ ISE-PIC รุ่น 3.2: ได้รับการแก้ไขแล้วใน Patch 8
- Cisco ISE หรือ ISE-PIC รุ่น 3.3: ได้รับการแก้ไขแล้วใน Patch 8
- Cisco ISE หรือ ISE-PIC รุ่น 3.4: ได้รับการแก้ไขแล้วใน Patch 4
- Cisco ISE หรือ ISE-PIC รุ่น 3.5: ยืนยันว่า ไม่ได้รับผลกระทบ

Cisco ระบุเพิ่มเติมว่า ไม่มีวิธีแก้ไขชั่วคราว (workaround) สำหรับช่องโหว่นี้ และยอมรับว่ามีโค้ด PoC ถูกเผยแพร่ออกมาแล้ว อย่างไรก็ตาม ในปัจจุบันยังไม่พบหลักฐานว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริงในระบบภายนอก

การแก้ไขช่องโหว่ในระบบ Snort 3

นอกจากนี้ Cisco ยังได้ออกแพตช์แก้ไขช่องโหว่ระดับปานกลางอีก 2 รายการ ซึ่งเกี่ยวข้องกับการประมวลผลคำสั่ง DCE/RPC โดยความเสี่ยงนี้อาจทำให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตน สามารถทำให้ Snort 3 Detection Engine เกิดการรั่วไหลของข้อมูลสำคัญ หรือถูกรีสตาร์ตระบบ ซึ่งจะส่งผลกระทบต่อการให้บริการของระบบโดยตรง

ช่องโหว่ทั้งสองนี้ถูกรายงานโดย Guy Lederfein นักวิจัยจาก Trend Micro โดยมีรายละเอียดดังนี้:

- CVE-2026-20026 (CVSS: 5.8): ช่องโหว่ประเภท Denial of Service (DoS) ใน Snort 3 จากการจัดการ DCE/RPC
- CVE-2026-20027 (CVSS: 5.3): ช่องโหว่การรั่วไหลของข้อมูลใน Snort 3 จากการจัดการ DCE/RPC

ผลิตภัณฑ์ของ Cisco ที่ได้รับผลกระทบประกอบด้วย:

- Cisco Secure Firewall Threat Defense (FTD) Software (ในกรณีที่ตั้งค่าใช้งาน Snort 3)
- Cisco IOS XE Software
- Cisco Meraki software

สรุปคำแนะนำ

เนื่องจากผลิตภัณฑ์ของ Cisco มักตกเป็นเป้าหมายของผู้ไม่หวังดีอยู่บ่อยครั้ง ผู้ใช้งานจึงควรอัปเดตระบบเป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบมีความปลอดภัยเพียงพอในการใช้งานและสามารถป้องกันความเสี่ยงจากช่องโหว่ต่างๆ ได้อย่างมีประสิทธิภาพ

ข้อมูลอ้างอิง

Jan 8, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/cisco-patches-ise-security.html