เอกสารแจ้งเตือนกรณีช่องโหว่ Zero-Day ใน Cisco ISE ถูกใช้โจมตี เสี่ยงข้ามการยืนยันตัวตนและเข้าควบคุมระบบ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ Zero-Day ใน Cisco ISE ถูกใช้โจมตี เสี่ยงข้ามการยืนยันตัวตนและเข้าควบคุมระบบ

พบรายงานการใช้ประโยชน์จากช่องโหว่ Zero-Day ใน Cisco Identity Services Engine (ISE) ซึ่งถูกนำไปใช้โจมตีจริง โดยช่องโหว่ดังกล่าวอาจทำให้ผู้โจมตีที่ไม่ได้รับอนุญาตสามารถ หลีกเลี่ยงการยืนยันตัวตน (Authentication Bypass) และเข้าถึงส่วนบริหารจัดการของระบบ Cisco ISE ได้ ส่งผลให้ผู้โจมตีอาจเข้าควบคุมระบบ เปลี่ยนแปลงการตั้งค่า หรือใช้เป็นช่องทางสำหรับโจมตีระบบเครือข่ายภายในองค์กรเพิ่มเติมได้[1]

โดย Cisco และหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ระบุว่า ช่องโหว่ดังกล่าวมีระดับความรุนแรงสูงสุด และพบการนำไปใช้โจมตีในสถานการณ์จริงแล้ว แนะนำให้ผู้ดูแลระบบเร่งตรวจสอบระบบที่ได้รับผลกระทบและติดตั้งซอฟต์แวร์แก้ไขโดยเร็วที่สุด เนื่องจากยังไม่มีมาตรการแก้ไขชั่วคราวที่สามารถทดแทนการอัปเดตได้[2]

<u>รายละเอียดช่องโหว่</u>

CVE-2026-76460(CVSS v3.1:10.0)[3] เป็นช่องโหว่ประเภท Authentication Bypass ใน Cisco Identity Services Engine (ISE) ช่องโหว่นี้เกิดจากการตรวจสอบสิทธิ์ของ API ภายในระบบไม่เพียงพอ ส่งผลให้ผู้โจมตีที่ไม่มีบัญชีผู้ใช้งาน สามารถส่งคำร้องขอที่ถูกสร้างขึ้นเป็นพิเศษเพื่อหลีกเลี่ยงการยืนยันตัวตนและเข้าถึง Web-based Management Interface ของ Cisco ISE ได้โดยไม่ได้รับอนุญาต

<u>รูปแบบการโจมตีและผลกระทบ</u>[4]

ผู้โจมตีจะค้นหาและมุ่งเป้าไปยังระบบ Cisco ISE ที่สามารถเข้าถึงได้ จากนั้นใช้ช่องโหว่ CVE-2026-76460 เพื่อข้ามกระบวนการยืนยันตัวตน และเข้าถึงส่วนบริหารจัดการของระบบโดยไม่ได้รับอนุญาต หากการโจมตีสำเร็จ อาจส่งผลกระทบดังนี้

1. ผู้โจมตีอาจสามารถเข้าถึงหน้าจัดการ Cisco ISE และดำเนินการที่ไม่ได้รับอนุญาตภายในระบบ
2. เปลี่ยนแปลงการตั้งค่าควบคุมการเข้าถึงเครือข่าย อาจส่งผลต่อการกำหนดสิทธิ์ผู้ใช้งาน อุปกรณ์ หรือการควบคุมการเชื่อมต่อภายในองค์กร
3. ผู้โจมตีอาจใช้สิทธิ์หรือข้อมูลที่ได้รับเพื่อขยายการเข้าถึงไปยังระบบอื่นเพิ่มเติม

ระบบที่ควรเฝ้าระวัง

1. ระบบที่ใช้งาน Cisco Identity Services Engine (ISE)
2. ระบบ Cisco ISE ที่เปิดให้เข้าถึงผ่านเครือข่ายที่ไม่ปลอดภัยหรือมีการเชื่อมต่อจากภายนอก
3. ระบบที่มีการใช้งาน Cisco ISE เป็นศูนย์กลางควบคุมสิทธิ์การเข้าถึงเครือข่าย (Network Access Control)

แนวทางการเฝ้าระวัง ป้องกัน และรับมือ

1. อัปเดต Cisco ISE เป็นเวอร์ชันที่ได้รับการแก้ไขทันที โดยตรวจสอบเวอร์ชันที่ใช้งานและติดตั้ง Software Update ตามคำแนะนำของ Cisco เพื่อป้องกันการถูกโจมตีจากช่องโหว่ดังกล่าว
2. ตรวจสอบ Log ของระบบ Cisco ISE เช่น access.log เพื่อค้นหาการเข้าถึงที่ผิดปกติ หรือความพยายามใช้งานบัญชี
3. ตรวจสอบการสร้างบัญชีใหม่ การเปลี่ยนแปลงสิทธิ์ การเข้าสู่ระบบที่ผิดปกติ และการแก้ไขค่าการตั้งค่าระบบโดยไม่ได้รับอนุญาต
4. จำกัดการเข้าถึงหน้า Management Interface ไม่ควรเปิดหน้า Web Management ของ Cisco ISE ให้เข้าถึงจากอินเทอร์เน็ตโดยตรง หากไม่มีความจำเป็น ควรจำกัดผ่าน VPN, IP Allowlist หรือเครือข่ายภายใน
5. เฝ้าระวังพฤติกรรมผิดปกติที่อาจเกิดขึ้นภายหลัง เช่น การเข้าถึงระบบภายใน การเปลี่ยนแปลงค่า Network Policy หรือการใช้งานบัญชีที่ผิดปกติ

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานหรือผู้ดูแลระบบที่ใช้งาน Cisco Identity Services Engine (ISE) ควรดำเนินการตรวจสอบระบบและติดตั้งแพตช์โดยเร็ว เนื่องจากช่องโหว่ดังกล่าวมีระดับความรุนแรงสูงสุดและพบการนำไปใช้โจมตีจริงแล้ว และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th

อ้างอิง

1. https://dg.th/9q4y85pd7x
2. https://dg.th/j18cmatwdh
3. https://dg.th/gjumbew6ks
4. https://dg.th/1utcy7amin