วันที่ 20 เมษายน 2569

## Cisco ออกแพตช์แก้ไขช่องโหว่ร้ายแรง 4 รายการใน Identity Services และ Webex ที่อาจนำไปสู่การรันโค้ดได้


Cisco ได้ประกาศแพตช์เพื่อแก้ไขช่องโหว่ด้านความปลอดภัยร้ายแรง 4 รายการ ที่ส่งผลกระทบต่อ Identity Services และ Webex Services ซึ่งอาจทำให้ผู้โจมตีสามารถรันโค้ดตามต้องการ และปลอมตัวเป็นผู้ใช้รายใดก็ได้ภายในระบบ

**รายละเอียดของช่องโหว่**

1. ช่องโหว่ CVE-2026-20184 (คะแนน CVSS: 9.8)

- สาเหตุ: เกิดจากการตรวจสอบใบรับรอง (Certificate) ไม่ถูกต้อง ในการเชื่อมต่อระบบล็อกอินแบบครั้งเดียว (Single Sign-On หรือ SSO) กับ Control Hub ใน Webex Services
- ผลกระทบ: อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ไม่ต้องยืนยันตัวตน สามารถปลอมเป็นผู้ใช้คนใดก็ได้ในระบบ และเข้าถึงบริการ Cisco Webex ได้โดยไม่ได้รับอนุญาต

2. ช่องโหว่ CVE-2026-20147 (คะแนน CVSS: 9.9)

- สาเหตุ: เป็นช่องโหว่ที่เกิดจากการตรวจสอบข้อมูลที่ผู้ใช้ป้อนไม่เพียงพอ ใน Identity Services Engine (ISE) และ ISE Passive Identity Connector (ISE-PIC)
- ผลกระทบ: อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่มีสิทธิ์ผู้ดูแลระบบ (Admin) สามารถรันโค้ดจากระยะไกลได้ โดยการส่งคำขอ HTTP ที่ถูกสร้างขึ้นมาเป็นพิเศษ

3. ช่องโหว่ CVE-2026-20180 และ CVE-2026-20186 (คะแนน CVSS: 9.9)

- สาเหตุ: เป็นช่องโหว่หลายรายการที่เกิดจากการตรวจสอบข้อมูลที่ผู้ใช้ป้อนไม่เพียงพอใน ISE
- ผลกระทบ: อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่มีสิทธิ์ผู้ดูแลแบบอ่านอย่างเดียว (Read-only admin) สามารถสั่งรันคำสั่งใดๆ บนระบบปฏิบัติการของอุปกรณ์ที่ได้รับผลกระทบได้ ผ่านการส่งคำขอ HTTP ที่ถูกสร้างขึ้นมาเป็นพิเศษ

  หากการโจมตีสำเร็จ ผู้โจมตีอาจสามารถเข้าถึงระบบปฏิบัติการในระดับผู้ใช้ และยกระดับสิทธิ์ขึ้นไปถึงระดับผู้ดูแลระบบสูงสุด (root) ได้

**ผลกระทบต่อเนื่อง: ภาวะปฏิเสธการให้บริการ (Denial of Service - DoS)**

Cisco กล่าวในประกาศเพิ่มเติมสำหรับช่องโหว่ CVE-2026-20147, CVE-2026-20180 และ CVE-2026-20186 ว่า

- ในกรณีที่ใช้งาน ISE แบบโหนดเดียว (Single-node) หากถูกโจมตีสำเร็จ อาจทำให้โหนด ISE ที่ได้รับผลกระทบไม่สามารถใช้งานได้ ส่งผลให้เกิดภาวะปฏิเสธการให้บริการ (Denial of Service หรือ DoS)
- ในช่วงเวลาดังกล่าว อุปกรณ์ที่ยังไม่ได้ยืนยันตัวตนจะไม่สามารถเข้าใช้งานเครือข่ายได้ จนกว่าจะมีการกู้คืนระบบ

**แนวทางการแก้ไขและการอัปเดตเวอร์ชัน**

การจัดการช่องโหว่ CVE-2026-20184 (Webex Services):

- สำหรับ CVE-2026-20184 ไม่จำเป็นต้องให้ผู้ใช้งานดำเนินการใดๆ เนื่องจากเป็นระบบแบบคลาวด์
- ข้อแนะนำเพิ่มเติม: ผู้ที่ใช้งานระบบ SSO แนะนำให้อัปโหลดใบรับรอง SAML ของผู้ให้บริการตัวตน (Identity Provider หรือ IdP) ใหม่ไปยัง Control Hub

การจัดการช่องโหว่อื่นๆ: ช่องโหว่ดังกล่าวได้รับการแก้ไขแล้วในซอฟต์แวร์เวอร์ชันดังต่อไปนี้

แพตช์สำหรับแก้ไข CVE-2026-20147

- Cisco ISE หรือ ISE-PIC เวอร์ชันก่อนหน้า 3.1: แนะนำให้อัปเกรดไปยังเวอร์ชันที่แก้ไขแล้ว
- Cisco ISE เวอร์ชัน 3.1: อัปเดตเป็น 3.1 Patch 11
- Cisco ISE เวอร์ชัน 3.2: อัปเดตเป็น 3.2 Patch 10
- Cisco ISE เวอร์ชัน 3.3: อัปเดตเป็น 3.3 Patch 11
- Cisco ISE เวอร์ชัน 3.4: อัปเดตเป็น 3.4 Patch 6
- Cisco ISE เวอร์ชัน 3.5: อัปเดตเป็น 3.5 Patch 3

แพตช์สำหรับแก้ไข CVE-2026-20180 และ CVE-2026-20186

- Cisco ISE เวอร์ชันก่อนหน้า 3.2: แนะนำให้อัปเกรดไปยังเวอร์ชันที่แก้ไขแล้ว
- Cisco ISE เวอร์ชัน 3.2: อัปเดตเป็น 3.2 Patch 8
- Cisco ISE เวอร์ชัน 3.3: อัปเดตเป็น 3.3 Patch 8
- Cisco ISE เวอร์ชัน 3.4: อัปเดตเป็น 3.4 Patch 4
- Cisco ISE เวอร์ชัน 3.5: ไม่พบช่องโหว่

แม้ว่า Cisco จะระบุว่ายังไม่พบการนำช่องโหว่เหล่านี้ไปใช้โจมตีจริงในขณะนี้ แต่ผู้ใช้งานควรอัปเดตระบบเป็นเวอร์ชันล่าสุดเพื่อความปลอดภัยสูงสุด

ข้อมูลอ้างอิง

Apr 16, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html