วันที่ 7 พฤศจิกายน 2568

ASD เตือนการโจมตี BADCANDY ที่ยังเกิดขึ้นต่อเนื่อง โดยอาศัยช่องโหว่ใน Cisco IOS XE

Australian Signals Directorate (ASD) ได้ออกประกาศเตือนภัยไซเบอร์ระดับสูง เกี่ยวกับการโจมตีอุปกรณ์ Cisco IOS XE ที่ยังไม่ได้ติดตั้งแพตช์ในออสเตรเลีย โดยมีจุดเด่นคือการใช้มัลแวร์รูปแบบใหม่ที่ไม่เคยถูกเปิดเผยมาก่อนในชื่อ BADCANDY

ช่องโหว่ร้ายแรง: CVE-2023-20198 (CVSS 10.0)

จากข้อมูลของหน่วยข่าวกรอง การโจมตีนี้เกี่ยวข้องกับการใช้ช่องโหว่ CVE-2023-20198 ซึ่งเป็นช่องโหว่ร้ายแรงระดับสูงสุด (CVSS: 10.0) ที่เปิดโอกาสให้แฮ็กเกอร์จากระยะไกลแบบไม่ต้องผ่านการยืนยันตัวตน (unauthenticated) สามารถสร้างบัญชีที่มีสิทธิ์สูง (privilege 15) และใช้บัญชีนั้นเข้าควบคุมระบบที่ยังมีช่องโหว่ได้

ช่องโหว่นี้ถูกนำมาใช้โจมตีจริงตั้งแต่ช่วงปลายปี 2023 โดยมีกลุ่มที่เชื่อมโยงกับจีน เช่น Salt Typhoon ใช้ช่องโหว่นี้เจาะระบบผู้ให้บริการโทรคมนาคมในช่วงหลายเดือนที่ผ่านมา

รู้จัก BADCANDY: เว็บเชลล์แบบ Lua ที่หลบซ่อน

ASD ระบุว่าพบรูปแบบต่าง ๆ ของ BADCANDY มาตั้งแต่เดือนตุลาคม 2023 และยังพบการโจมตีชุดใหม่อย่างต่อเนื่องในปี 2024 และ 2025 โดยมีอุปกรณ์ในออสเตรเลียมากถึง 400 เครื่อง ที่ถูกเจาะตั้งแต่เดือนกรกฎาคม 2025 โดย 150 เครื่อง ถูกติดตั้งมัลแวร์ในเดือนตุลาคมเดือนเดียว

“BADCANDY เป็น เว็บเชลล์แบบ Lua ที่มีขนาดเล็ก และผู้โจมตีมักจะติดตั้งแพตช์แบบไม่ถาวร หลังจากเจาะระบบสำเร็จ เพื่อทำให้ดูเหมือนว่าอุปกรณ์ไม่ได้มีช่องโหว่เกี่ยวกับ CVE-2023-20198” หน่วยงานระบุ “ในสถานการณ์เหล่านี้ การพบ BADCANDY บ่งชี้ว่าอุปกรณ์ Cisco IOS XE ถูกเจาะผ่านช่องโหว่ CVE-2023-20198 แล้ว”

- ข้อจำกัดและความเสี่ยงการโจมตีซ้ำ: แม้มัลแวร์นี้จะไม่มีความสามารถในการคงอยู่ถาวร (persistence) และจะหายไปหลังรีบูตเครื่อง แต่ถ้าอุปกรณ์ยังคงไม่ได้แพตช์และเปิดให้เข้าถึงผ่านอินเทอร์เน็ต ผู้โจมตีก็สามารถนำมัลแวร์กลับมาวางใหม่และยึดการเข้าถึงคืนได้อีกครั้ง
- การโจมตีซ้ำที่เกิดขึ้นจริง: ASD ประเมินว่าผู้โจมตีสามารถตรวจจับได้เมื่อมีการลบ implant ออกไป และจะกลับมาติดตั้งใหม่ โดยพบการโจมตีซ้ำบนอุปกรณ์ที่ ASD เคยแจ้งเตือนเจ้าของระบบไปก่อนหน้านี้แล้ว

แนวทางปฏิบัติเพื่อป้องกันและตรวจสอบการถูกเจาะระบบ

อย่างไรก็ตามการรีบูตเครื่องจะไม่ลบการเปลี่ยนแปลงอื่น ๆ ที่ผู้โจมตีทำไว้ ดังนั้นผู้ดูแลระบบจึงจำเป็นต้องติดตั้งแพตช์ จำกัดการเปิดเผยหน้าเว็บอินเทอร์เฟซสู่สาธารณะ และทำตามแนวทางการเพิ่มความปลอดภัยตามที่ Cisco แนะนำเพื่อป้องกันไม่ให้ถูกเจาะซ้ำในอนาคต

คำแนะนำเพิ่มเติมจาก ASD สำหรับผู้ดูแลระบบ:

1. **ตรวจสอบบัญชีผู้ใช้:**
    - ตรวจสอบค่า running configuration เพื่อค้นหาบัญชีที่มีสิทธิ์ระดับ privilege 15 และลบบัญชีที่ไม่คาดคิดหรือไม่ได้รับอนุญาต
    - ตรวจสอบบัญชีที่มีชื่อเป็นชุดตัวอักษรแปลก ๆ หรือชื่อ “cisco_tac_admin,” “cisco_support,” “cisco_sys_manager,” หรือ “cisco” และลบออกหากไม่ใช่บัญชีที่ถูกต้อง
2. **ตรวจสอบการตั้งค่าเครือข่าย:**
    - ตรวจสอบค่า running configuration สำหรับ tunnel interfaces ที่ไม่รู้จัก
3. **ตรวจสอบบันทึก (Logging):**
    - ตรวจสอบ TACACS+ AAA command accounting logging เพื่อดูการเปลี่ยนแปลงการตั้งค่า (หากมีการเปิดใช้งานไว้)

ข้อมูลอ้างอิง

Nov 1, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/11/asd-warns-of-ongoing-badcandy-attacks.html