วันที่ 26 กันยายน 2568

## Cisco ASA Zero-Day Duo ถูกโจมตี CISA ออกคำสั่งบรรเทาฉุกเฉิน


Cisco ได้เรียกร้องให้ลูกค้าดำเนินการอัปเดตแก้ไขช่องโหว่ด้านความปลอดภัย 2 จุดที่กระทบต่อ VPN web server ของซอฟต์แวร์ Cisco Secure Firewall Adaptive Security Appliance (ASA) และ Cisco Secure Firewall Threat Defense (FTD) เนื่องจากทางบริษัทระบุว่า ช่องโหว่เหล่านี้ถูกนำไปใช้โจมตีจริงแล้ว

**รายละเอียดช่องโหว่ Zero-Day ที่มีการโจมตี**

ช่องโหว่ร้ายแรงที่ถูกนำมาใช้โจมตีมีดังนี้:

- CVE-2025-20333 (คะแนน CVSS: 9.9):
    - เป็นช่องโหว่ที่มีความรุนแรงสูงมาก เกิดจากการตรวจสอบข้อมูลที่ผู้ใช้ส่งเข้ามาในคำขอ HTTP(S) ไม่ถูกต้อง (Improper input validation)
    - อนุญาตให้ผู้โจมตีจากระยะไกลที่ มีบัญชี VPN ถูกต้อง สามารถรันโค้ดอันตรายในสิทธิ์ root บนเครื่องที่ได้รับผลกระทบได้ เพียงแค่ส่งคำขอ HTTP ที่ถูกสร้างขึ้นมาเฉพาะ
- CVE-2025-20362 (คะแนน CVSS: 6.5):
    - เป็นช่องโหว่การตรวจสอบข้อมูลที่ผู้ใช้ส่งเข้ามาในคำขอ HTTP(S) ไม่ถูกต้องเช่นกัน
    - อนุญาตให้ผู้โจมตีจากระยะไกลที่ ไม่ต้องมีบัญชีใด ๆ สามารถเข้าถึง URL ที่ควรจำกัดสิทธิ์ไว้ได้ เพียงแค่ส่งคำขอ HTTP ที่สร้างขึ้นมา

Cisco กล่าวว่าทราบถึง “ความพยายามในการโจมตี” ช่องโหว่ทั้งสองแล้ว และคาดการณ์ว่าช่องโหว่ทั้งสองถูกนำมา เชื่อมต่อกัน เพื่อข้ามขั้นตอนการยืนยันตัวตนและรันโค้ดอันตรายบนอุปกรณ์ที่มีช่องโหว่ บริษัทได้ขอบคุณหน่วยงานความมั่นคงหลายแห่ง เช่น ACSC (ออสเตรเลีย), Canadian Centre for Cyber Security, NCSC (สหราชอาณาจักร) และ CISA (สหรัฐฯ) ที่สนับสนุนการสืบสวน

**CISA ออกคำสั่งฉุกเฉินรับมือ ArcaneDoor**

ในประกาศแยกต่างหาก CISA (Cybersecurity and Infrastructure Security Agency) ได้ออก คำสั่งฉุกเฉิน (Emergency Directive - ED 25-03) เพื่อกระตุ้นให้หน่วยงานรัฐบาลกลางรีบระบุ วิเคราะห์ และบรรเทาผลกระทบที่อาจเกิดขึ้นทันที นอกจากนี้ ช่องโหว่ทั้งสองยังถูกเพิ่มเข้าไปในบัญชี Known Exploited Vulnerabilities (KEV) catalog ซึ่งบังคับให้หน่วยงานต่างๆ ต้องอัปเดตแก้ไขภายใน 24 ชั่วโมง

CISA ยืนยันว่า “CISA ทราบถึงแคมเปญการโจมตีที่กำลังดำเนินอยู่โดยแฮกเกอร์ขั้นสูงที่มุ่งเป้าไปที่ Cisco Adaptive Security Appliances (ASA)” โดยเน้นย้ำถึงความรุนแรงของการโจมตี:

1. การรันโค้ดระดับสูง: มีการใช้ช่องโหว่ Zero-Day เพื่อให้ได้สิทธิ์ รันโค้ดจากระยะไกลโดยไม่ต้องล็อกอิน
2. การฝังตัวอย่างถาวร: แฮกเกอร์มีการ แก้ไขหน่วยความจำแบบ read-only (ROM) เพื่อให้ฝังตัวอยู่ได้แม้จะมีการรีบูตหรืออัปเกรดระบบ การกระทำนี้สร้างความเสี่ยงอย่างมากต่อเครือข่ายที่ตกเป็นเป้าหมาย

CISA กล่าวเพิ่มเติมว่ากิจกรรมดังกล่าวเชื่อมโยงกับกลุ่มภัยคุกคามที่เรียกว่า ArcaneDoor ซึ่งเคยถูกระบุว่าโจมตีอุปกรณ์เครือข่ายจากหลายผู้ผลิต รวมถึง Cisco เพื่อส่งมัลแวร์ตระกูล Line Runner และ Line Dancer กิจกรรมนี้ถูกโยงไปถึงแฮกเกอร์ที่ใช้ชื่อว่า UAT4356 (หรือ Storm-1849)

“แฮกเกอร์กลุ่มนี้ได้แสดงให้เห็นแล้วว่าสามารถแก้ไข ROM ของ ASA ได้สำเร็จตั้งแต่ช่วงต้นปี 2024” CISA กล่าวเสริม “ช่องโหว่ Zero-Day บนแพลตฟอร์ม Cisco ASA ยังพบในบางเวอร์ชันของ Cisco Firepower ด้วย ซึ่งในอุปกรณ์ Firepower ระบบ Secure Boot จะสามารถตรวจจับการแก้ไข ROM ที่พบได้”

ภัยคุกคามนี้รุนแรงและถูกใช้โจมตีจริงโดยกลุ่มแฮกเกอร์ขั้นสูง การอัปเดตแพตช์ล่าสุดสำหรับ Cisco ASA และ FTD จึงเป็นเรื่องเร่งด่วนที่สุด

**ข้อมูลอ้างอิง**

**Sep 25, 2025, By Ravie Lakshmanan**

- https://thehackernews.com/2025/09/urgent-cisco-asa-zero-day-duo-under.html