ประจำวันศุกร์ที่ 5 สิงหาคม 2565

Cisco Business Routers พบช่องโหว่ที่สำคัญต่อการถูกโจมตีจากระยะไกล

เมื่อวันพุธที่ผ่านมา Cisco ได้เปิดตัวแพตช์เพื่อแก้ไขช่องโหว่ด้านความปลอดภัยจำนวน 8 จุด โดยมี 3 ช่องโหว่ที่อาจถูกโจมตีจากผู้โจมตีโดยที่ไม่ผ่านการตรวจสอบสิทธิ์เพื่อการเรียกใช้โค้ดจากระยะไกล (RCE) หรือทำให้เกิดเงื่อนไขการปฏิเสธบริการ (DoS) บนอุปกรณ์ที่ได้รับผลกระทบ

ช่องโหว่ที่สำคัญที่สุดส่งผลกระทบต่อ Routers รุ่น Cisco Small Business RV160, RV260, RV340 และ RV345 Series โดยหมายเลขช่องโหว่ CVE-2022-20842 (คะแนน CVSS : 9.8) เกิดจากการตรวจสอบข้อมูลที่ผู้ใช้จัดหาไม่เพียงพอไปยังอินเทอร์เฟซการจัดการบนเว็บของอุปกรณ์

ช่องโหว่ที่ 2 เกี่ยวข้องกับช่องโหว่ในการแทรกคำสั่งที่อยู่ในลักษณะการอัปเดตฐานข้อมูลตัวกรองเว็บของ Routers โดยหมายเลขช่องโหว่ (CVE-2022-20827 คะแนน CVSS : 9.0) ซึ่งทำให้ฝ่ายผู้โจมตีสามารถเจาะระบบและดำเนินการคำสั่งตามอำเภอใจบนระบบปฏิบัติการพื้นฐาน ด้วยสิทธิ์รูท

ช่องโหว่ที่ 3 เกี่ยวข้องกับ Routers หมายเลขช่องโหว่ (CVE-2022-20841 คะแนน CVSS : 8.0) เป็นช่องโหว่การ injection ในโมดูล Open Plug-n-Play (PnP) ที่อาจถูกใช้ในการส่งข้อมูลที่เป็นอันตรายเพื่อให้สามารถ รันโค้ดบนโฮสต์ Linux เป้าหมายได้

นอกจากนี้ Cisco ยังแก้ไขช่องโหว่ด้านความปลอดภัยระดับกลาง 5 รายการซึ่งส่งผลต่อ Webex Meetings, Identity Services Engine, Unified Communications Manager และ BroadWorks Application Delivery Platform แต่ยังไม่มีหลักฐานว่าช่องโหว่เหล่านี้ถูกนำไปใช้ประโยชน์ ซึ่ง Cisco แนะนำให้ลูกค้าควรอัปอย่างเร็วที่สุด

ที่มาของข่าว : https://thehackernews.com/2022/08/cisco-business-routers-found-vulnerable.html