

ประจำวันอังคารที่ 24 พฤษภาคม 2565

# Cisco ออก Patch สำหรับ IOS XR Zero-Day Vulnerability ใหม่

Cisco ได้เปิดตัวโปรแกรมแก้ไขสำหรับช่องโหว่ที่มีความรุนแรงปานกลาง ซึ่งส่งผลกระทบต่อซอฟต์แวร์ IOS XR โดยระบุว่าการใช้ช่องโหว่ในการโจมตี หมายเลข CVE-2022-20821 (คะแนน CVSS: 6.5) ปัญหานี้เกี่ยวข้องกับช่องโหว่พอร์ตเปิดที่อาจถูกใช้ในทางที่ผิดโดยผู้โจมตีจากระยะไกลที่ไม่ผ่านการตรวจสอบสิทธิ์เพื่อเชื่อมต่อกับ Redis instance และการเรียกใช้ code execution "การเจาะระบบที่ประสบความสำเร็จอาจทำให้ผู้โจมตีสามารถเขียนฐานข้อมูลในหน่วยความจำ Redis เขียนไฟล์โดยอำเภอใจไปยังระบบไฟล์คอนเทนเนอร์ และดึงข้อมูลเกี่ยวกับฐานข้อมูล Redis" Cisco กล่าวในคำแนะนำ "ด้วยการกำหนดค่าคอนเทนเนอร์ แชนด์บ็อกซ์ที่ Redis instance ทำงาน ผู้โจมตีจากระยะไกลจะไม่สามารถเรียกใช้โค้ดจากระยะไกลหรือใช้คุณสมบัติของระบบโฮสต์ Cisco IOS XR Software ในทางที่ผิด" บ็อกกพร่องดังกล่าว ซึ่งระบุได้ในระหว่างการแก้ไขกรณีของศูนย์ช่วยเหลือด้านเทคนิค (TAC) ส่งผลกระทบต่อเราเตอร์ Cisco 8000 Series ที่รันซอฟต์แวร์ IOS XR มีการติดตั้ง RPM การตรวจสอบสภาพและทำงานอยู่โดยผู้พลิตอุปกรณ์เครือข่ายยังทราบถึงการพยายามใช้ประโยชน์จากจุดบกพร่องนี้เมื่อต้นเดือน และขอแนะนำอย่างยิ่งให้ลูกค้าใช้วิธีแก้ปัญหที่เหมาะสมหรืออัปเดตซอฟต์แวร์เพื่อแก้ไขช่องโหว่นี้

