ประจำวันศุกร์ที่ 9 กันยายน 2565

Cisco ออกแพทช์ความปลอดภัยสำหรับช่องโหว่ใหม่ที่ส่งผลกระทบต่อหลายผลิตภัณฑ์

เมื่อวันพุธที่ผ่านมา Cisco ได้เปิดตัวแพทช์เพื่อแก้ไขช่องโหว่ความปลอดภัยสามรายการที่ ส่งผลต่อผลิตภัณฑ์ของบริษัท ซึ่งรวมถึงจุดอ่อนที่มีความรุนแรงสูงที่ถูกเปิดเผยใน NVIDIA Data Plane Development Kit (MLNX_DPDK) เมื่อปลายเดือนที่แล้ว

หมายเลขช่องโหว่แรก CVE-2022-28199 (คะแนน CVSS: 8.6) ช่องโหว่นี้เกิดจากการขาดการจัดการข้อผิดพลาดที่เหมาะสมในเครือข่าย stack ของ DPDK ทำให้ผู้โจมตีระยะไกลสามารถทริกเกอร์เงื่อนไขการปฏิเสธบริการ (DoS) และก่อให้เกิดผลกระทบต่อ ความสมบูรณ์ของข้อมูลและการรักษาความลับ โดยที่ DPDK คือชุดของไลบรารีและไดรเวอร์การ์ดเชื่อมต่อเครือข่าย (NIC) ที่ปรับให้เหมาะสมสำหรับการประมวลผลแพ็กเก็ตที่รวดเร็ว โดยมีกรอบงานและ API ทั่วไปสำหรับแอปพลิเคชันเครือข่ายความเร็วสูง

Cisco กล่าวไว้ว่าได้ตรวจสอบกลุ่มผลิตภัณฑ์เพื่อพิจารณาถึงผลกระทบจากช่องโหว่ และแนะนำให้ผู้ผลิตอุปกรณ์เครือข่ายออกการอัปเดตซอฟต์แวร์ ดังต่อไปนี้
-Cisco Catalyst 8000V Edge Software
-Adaptive Security Virtual Appliance (ASAv)
-Secure Firewall Threat Defense Virtual (formerly FTDv)

หมายเลขช่องโหว่ที่สอง CVE-2022-20696 (คะแนน CVSS: 7.5) เกิดจากไม่มีการป้องกันที่เพียงพอในพอร์ตคอนเทนเนอร์ของเซิร์ฟเวอร์การส่งข้อความ หากการใช้ประโยชน์จากช่องโหว่ประสบความสำเร็จอาจทำให้ผู้โจมตีสามารถเห็นและแทรกข้อความลงในบริการส่งข้อความ ซึ่งอาจทำให้เกิดการเปลี่ยนแปลงการกำหนดค่าหรือทำให้ระบบโหลดซ้ำ

หมายเลขช่องโหว่ที่สาม CVE-2022-20863 คะแนน (CVSS: 4.3) คือช่องโหว่ในอินเทอร์เฟซการส่งข้อความของ Cisco Webex App ซึ่งสามารถเปิดใช้งานจากผู้โจมตีระยะไกลที่ไม่ผ่านการตรวจสอบสิทธิ์เพื่อแก้ไขลิงก์หรือเนื้อหาอื่น ๆ และสามารถดำเนินการโจมตีแบบ Phishing

Cisco ให้เครดิต Rex, Bruce และ Zachery จาก Binance Red Team สำหรับการค้นพบและรายงานช่องโหว่ ซึ่งสุดท้ายนี้ยังเปิดเผยรายละเอียดของบั๊กบายพาสที่หมายเลขช่องโหว่ CVE-2022-20923 (คะแนน CVSS: 4.0) ที่ส่งผลกระทบต่อเราเตอร์ Cisco Small Business RV110W, RV130, RV130W และ RV215W ซึ่งระบุว่าจะไม่ได้รับการแก้ไขเนื่องจากผลิตภัณฑ์ใกล้จะสิ้นสุด

ที่มาของข่าว : https://thehackernews.com/2022/09/cisco-releases-security-patches-for-new.html