ประจำวันจันทร์ที่ 15 สิงหาคม 2565

Cisco ออก แพตช์แก้ไขช่องโหว่ที่มีความรุนแรงสูง ที่ส่งผลต่อ ASA และ Firepower Solutions

เมื่อวันพุธที่ผ่านมา Cisco ได้ออกแพตช์เพื่อแก้ไขช่องโหว่หลายอย่างในซอฟต์แวร์ของ Cisco ซึ่งช่องโหว่นี้อาจทำให้มีข้อมูลสำคัญรั่วไหลออกไปบนอุปกรณ์ที่มีความ sensitive หมายเลขช่องโหว่ CVE-2022-20866 (คะแนน CVSS : 7.4) ซึ่งได้รับการอธิบายว่าเป็น "logic error" เมื่อจัดการคีย์ RSA บนอุปกรณ์ที่ใช้ซอฟต์แวร์ Cisco Adaptive Security Appliance (ASA) และ Cisco Firepower Threat Defense (FTD) ซอฟต์แวร์ ทำให้การใช้ประโยชน์จากช่องโหว่ สำเร็จอาจทำให้ผู้โจมตีสามารถเรียกค้นคีย์ส่วนตัว RSA ได้โดยใช้ช่องทางด้านข้างของ Lenstra โจมตีอุปกรณ์เป้าหมาย

Cisco ตั้งข้อสังเกตว่าช่องโหว่ดังกล่าวได้ส่งผลกระทบเฉพาะซอฟต์แวร์ Cisco ASA เวอร์ชั่น 9.16.1 และใหม่กว่า และซอฟต์แวร์ Cisco FTD เวอร์ชั่น 7.0.0 และใหม่กว่า โดยมีผลิตภัณฑ์ที่ได้รับผลกระทบดังนี้
-ASA 5506-X with FirePOWER Services
-ASA 5506H-X with FirePOWER Services
-ASA 5506W-X with FirePOWER Services
-ASA 5508-X with FirePOWER Services
-ASA 5516-X with FirePOWER Services
-Firepower 1000 Series Next-Generation Firewall
-Firepower 2100 Series Security Appliances
-Firepower 4100 Series Security Appliances
-Firepower 9300 Series Security Appliances, and
-Secure Firewall 3100

นอกจากนี้ Cisco ยังปรับปรุงแก้ไขช่องโหว่การลักลอบขอคำขอฝั่งไคลเอ็นต์ในคอมโพเนนต์ Clientless SSL VPN (WebVPN) ของซอฟต์แวร์ Cisco Adaptive Security Appliance (ASA) ที่สามารถเปิดใช้งานให้ผู้โจมตีจากระยะไกลที่ไม่ผ่านการตรวจสอบสิทธิ์เพื่อดำเนินการโจมตีบนเบราว์เซอร์ เช่น cross-site scripting บริษัทกล่าวว่าช่องโหว่ CVE-2022-20713 (คะแนน CVSS : 4.3) ยังได้ส่งผลกระทบต่ออุปกรณ์ Cisco ที่ใช้งานซอฟต์แวร์ Cisco ASA Software รุ่นก่อนหน้า 9.17(1) และเปิดใช้งานคุณลักษณะ Clientless SSL VPN

บริษัทรักษาความปลอดภัยทางไซเบอร์ Rapid7 เปิดเผยรายละเอียดช่องโหว่ 10 รายการที่พบใน ASA, Adaptive Security Device Manager (ASDM) และซอฟต์แวร์บริการ FirePOWER สำหรับ ASA ซึ่ง Cisco ได้แก้ไขไปแล้ว 7 รายการ

ที่มาของข่าว : https://thehackernews.com/2022/08/cisco-patches-high-severity.html