วันที่ 3 เมษายน 2567

Cisco addressed multiple vulnerabilities in IOS and IOS XE software that can be exploited to trigger a denial-of-service (DoS) condition

Executive Summary

ทางศูนย์ CSOC พบรายงานการแจ้งเตือนเกี่ยวกับช่องโหว่ในซอฟต์แวร์ IOS และ IOS XE ที่สามารถใช้ประโยชน์เพื่อเรียกใช้การปฏิเสธการให้บริการ (DoS) โดย Cisco ได้ปล่อยแพทช์ไปยังที่อยู่ช่องโหว่ของซอฟต์แวร์ IOS และ IOS XE หลายรายการ ซึ่งผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถใช้ประโยชน์จากปัญหาต่างๆ ที่แก้ไขโดยยักษ์ใหญ่ด้านไอทีเพื่อทำให้เกิดเงื่อนไขการปฏิเสธการให้บริการ (DoS)

CVE details

- CVE-2024-20311 (CVSS score 8.6) เป็นช่องโหว่ในคุณสมบัติ Locator ID Separation Protocol (LISP) ของซอฟต์แวร์ Cisco IOS และซอฟต์แวร์ IOS XE ทำให้ผู้โจมตีระยะไกลที่ไม่ผ่านการตรวจสอบความถูกต้องผ่านทางช่องโหว่ที่ทำให้อุปกรณ์ที่ได้รับผลกระทบซ้ำ
- CVE-2024-20314 (CVSS score 8.6) เป็นช่องโหว่ใน IPv4 Software-Defined Access (SD-Access) ของ Cisco IOS XE Software ทำให้ผู้โจมตีระยะไกลที่ไม่ผ่านการตรวจสอบความถูกต้องผ่านทางช่องโหว่ที่ทำให้เกิดการใช้ CPU สูงและหยุดการประมวลผลทราฟฟิกทั้งหมดส่งผลให้สภาพการปฏิเสธบริการ (DoS)
- CVE-2024-20307 – CVE-2024-20308 (CVSS score 8.6) เป็นช่องโหว่หลายจุดในคุณสมบัติการกระจายตัวของ Internet Key Exchange เวอร์ชั่น 1 (IKEv1) ของ Cisco IOS และ Cisco IOS XE ทำให้ผู้โจมตีอนุญาตให้ดำเนินการโจมตีแบบ RCE ที่ไม่ได้รับการรับรองความถูกต้องทำให้เกิดความเสียหายในระบบที่ได้รับผลกระทบ
- CVE-2024-20259 (CVSS score 8.6) เป็นช่องโหว่ที่มคุณสมบัติ DHCP snooping ของซอฟต์แวร์ Cisco IOS XE ทำให้ผู้โจมตีระยะไกลที่ไม่ผ่านการตรวจสอบความถูกต้องสามารถดำเนินการโจมตีผ่านช่องโหว่เพื่อให้อุปกรณ์ที่ได้รับผลกระทบโหลดซ้ำโดยไม่คาดคิด ส่งผลให้สภาพการปฏิเสธบริการ (DoS)
- CVE-2024-20303 (CVSS score 7.4) เป็นช่องโหว่ในคุณสมบัติเกตเวย์ Multicast DNS (mDNS) ของซอฟต์แวร์ Cisco IOS XE สำหรับคอนโทรลเลอร์ LAN ไร้สาย (WLCs) ทำให้ผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถดำเนการโจมตีผ่านช่องโหว่ เพื่อทำให้เกิดเงื่อนไขการปฏิเสธการให้บริการ (DoS)

ศูนย์ CSOC แนะนำให้ลูกค้าตรวจสอบรายละเอียดด้านความปลอดภัยของ IOS และ IOS XE software ที่ใช้ภายในองค์กรรวมถึงตรวจสอบความผิดปกติที่อาจเกิดขึ้นซึ่งเป็นความเสี่ยงที่อาจทำให้เกิดการโจมตีและเพื่อลดความเสี่ยงที่อาจเกิดขึ้น โดยช่องโหว่นี้เป็นช่องโหว่ที่ก่อให้เกิดความเสี่ยงที่ยอมรับไม่ได้ต่อองค์กรควรต้องมีการดำเนินการตรวจสอบเพื่อลดความเสี่ยง ทั้งนี้ในช่วงเวลาที่รายงานฉบับนี้ออก (28 มี.ค. 2567) และยังไม่พบ Proof-of-concept code สำหรับการโจมตีช่องโหว่นี้และยังพบรายงานเกี่ยวกับการโจมตีช่องโหว่เหล่านี้ในอินเทอร์เน็ต

รายละเอียดของช่องโหว่โดยสรุป

- ผลิตภัณฑ์ที่ได้รับผลกระทบ: CISCO Software
- หน่วยงานที่ออกคำแนะนำด้านความปลอดภัย: IOS และ IOS XE software
- ผลกระทบ (Impact): DOS, RCE
- CVE Name:
    - CVE-2024-20311 (CVSS score 8.6)
    - CVE-2024-20314 (CVSS score 8.6)
    - CVE-2024-20307 – CVE-2024-20308 (CVSS score 8.6)
    - CVE-2024-20259 (CVSS score 8.6)
    - CVE-2024-20303 (CVSS score 7.4)
- การแก้ไขปัญหา:
    - ทำการอัพเดต Cisco IOS และ IOS XE โดยใช้เวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่แล้ว
    - ตรวจสอบความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่และวิเคราะห์ผลกระทบที่อาจเกิดขึ้นกับระบบ
    - การกำหนดค่าของระบบเพื่อลดความเสี่ยงหรือป้องกันการโจมตีจากช่องโหว่ เช่น การกำหนดค่า ACL (Access Control Lists) เพื่อควบคุมการเข้าถึง
    - การติดตามและการควบคุมการเข้าถึงการใช้งานที่ไม่ปกติหรือการโจมตีที่เป็นไปได้

ข้อมูลที่พบจาก Threat intelligence

- ในช่วงเวลาที่รายงานฉบับนี้ออก (28 มี.ค. 2567) ยังพบ Proof-of-concept code สำหรับการโจมตีช่องโหว่นี้และยังพบรายงานเกี่ยวกับการโจมตีช่องโหว่เหล่านี้ในอินเทอร์เน็ต

ทั้งนี้การแก้ไข Configuration เพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว ลูกค้าควรปฏิบัติตาม Change Management Policy หรือ Risk Management Policy หรือ Business Impact Assessment ของหน่วยงานอย่างเคร่งครัด

ข้อมูลอ้างอิง

- https://securityaffairs.com/161181/security/cisco-ios-and-ios-xe-software-flaws.html