แจ้งเตือน : ช่องโหว่

High

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [ ] Loss of Integrity
- [ ] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือนช่องโหว่ระดับสูงของผลิตภัณฑ์ Cisco (CVE-2024-20259, CVE-2024-20303, CVE-2024-20307, CVE-2024-20311 และ CVE-2024-20314)

วันที่แจ้งเตือน 12 เมษายน 2567

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ผลกระทบระดับสูงในผลิตภัณฑ์ **Cisco** รวมจำนวน 6 รายการ มีรายละเอียดดังนี้

| CVE | Description | Affected |
|---|---|---|
| CVE-2024-20259 | ช่องโหว่บนฟีเจอร์ DHCP snooping ที่เปิดใช้งาน “endpoint analytics” ของซอฟต์แวร์ IOS XE มีการจัดการผิดพลาดกับ crafted IPv4 DHCP request ที่สร้างขึ้นโดยผู้ไม่หวังดี และจะส่ง request ดังกล่าวไปยังอุปกรณ์ที่มีช่องโหว่ ส่งผลให้อุปกรณ์สามารถให้บริการได้ | • Catalyst 9000 Series Switches<br>• DNA Traffic Telemetry Appliance |
| CVE-2024-20303 | ช่องโหว่บนฟีเจอร์ multicast DNS (mDNS) gateway ของซอฟต์แวร์ IOS XE ในอุปกรณ์ Wireless LAN Controllers (WLCs) มีการจัดการผิดพลาดกับอุปกรณ์ที่มาเรียกใช้งาน mDNS ทำให้ผู้ไม่หวังดีสามารถเชื่อมต่อกับเครือข่ายไร้สายและส่งข้อมูล mDNS packet ที่เฉพาะเจาะจงอย่างต่อเนื่อง ทำให้ CPU ของ WLCs มีการใช้งานสูง ส่งผลให้ WLCs ไม่สามารถให้บริการได้ | • Catalyst 9800-CL Wireless Controllers for Cloud<br>• Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches<br>• Catalyst 9800 Series Wireless Controllers<br>• Embedded Wireless Controller on Catalyst APs |
| CVE-2024-20307 และ CVE-2024-20308 | ช่องโหว่บนฟีเจอร์ Internet Key Exchange Version 1 (IKEv1) fragmentation ของซอฟต์แวร์ IOS และ IOS XE ทำให้ผู้ไม่หวังดีจากระยะไกลสามารถโจมตีหน่วยความจำ (heap overflow) ส่งผลให้อุปกรณ์ไม่สามารถให้บริการได้ | Cisco IOS หรือ IOS XE ที่เปิดใช้งานทั้ง 2 ฟีเจอร์ดังนี้<br>• IKEv1 fragmentation และ<br>• Any type of VPN that is based on IKEv1 is configured |
| CVE-2024-20311 | ช่องโหว่บนฟีเจอร์ Locator ID Separation Protocol (LISP) ของซอฟต์แวร์ IOS และ IOS XE ช่องโหว่นี้เกิดจากการจัดการ LISP ที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีส่ง LISP packet ไปยังอุปกรณ์ที่มีช่องโหว่ ส่งผลให้อุปกรณ์ไม่สามารถให้บริการได้ | Cisco IOS หรือ IOS XE ที่เปิดใช้งาน LISP และมีการใช้งานคำสั่ง<br>• Ingress/egress tunnel router หรือ<br>• Map server หรือ<br>• Map resolver |
| CVE-2024-20314 | ช่องโหว่บนฟีเจอร์ IPv4 Software-Defined Access (SD-Access) fabric edge ของซอฟต์แวร์ IOS XE ช่องโหว่นี้เกิดจากการจัดการ IPv4 packet ที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดี ส่ง IPv4 packet ไปยังอุปกรณ์ที่มีช่องโหว่ ส่งผลให้อุปกรณ์ไม่สามารถให้บริการได้ | Cisco IOS XE ที่มีการตั้งค่าการใช้งานให้ทำหน้าที่เป็น SD-Access fabric edge nodes |

ทั้งนี้ Cisco มีการออก Patch แก้ไขช่องโหว่ดังกล่าวแล้ว และ แนะนำให้ผู้ใช้งานทำการอัปเดตซอฟตแวร เปนเวอรชันล่าสุดทันที

**ข้อมูลอ้างอิง**


1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 11 เม.ย. 2567
2) https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities
3) https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-034