แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : CLEAR
☒ Financial Damage ☒ Reputation Damage ☒ Non-compliance ☒ Privacy Violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ความรุนแรงระดับวิกฤต และ ระดับสูงหลายรายการ ของผลิตภัณฑ์ Cisco IOS และ IOS XE

วันที่แจ้งเตือน 22 พฤษภาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานช่องโหว่ความรุนแรงระดับวิกฤต และระดับสูง จำนวนหลายรายการของผลิตภัณฑ์ Cisco ซึ่งเป็นช่องโหว่ของซอฟต์แวร์ Cisco IOS และ IOS XE โดยเป็นช่องโหว่ความรุนแรงระดับวิกฤต จำนวน 1 รายการ ระดับสูง จำนวน 16 รายการ และ ระดับปานกลาง จำนวน 16 รายการ โดย Cisco ได้ออกซอฟต์แวร์แก้ไขช่องโหว่เหล่านี้แล้ว

ทั้งนี้ ช่องโหว่ความรุนแรงระดับวิกฤตเป็นช่องโหว่ในฟีเจอร์ Out-of-Band Access Point (AP) Image Download ของ Cisco IOS XE Software สำหรับ Wireless LAN Controllers (WLCs) ซึ่งผู้ไม่หวังดีอาจใช้เพื่ออัปโหลดไฟล์ไปยังระบบผ่านการส่งคำขอ HTTPS ที่ถูกสร้างขึ้น และ เรียกใช้คำสั่งด้วยสิทธิ root ในระบบได้

ThaiCERT แนะนำให้ผู้ดูแลระบบ และผู้ใช้งานผลิตภัณฑ์ Cisco ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน

Vulnerabilities	Affected Products	Solution
ระดับ Critical 1 รายการ ได้แก่ CVE-2025-20188: Cisco IOS XE Wireless Controller Software Arbitrary File Upload Vulnerability	• Catalyst 9800-CL Wireless Controllers for Cloud • Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches • Catalyst 9800 Series Wireless Controllers • Embedded Wireless Controller on Catalyst APs ** โดยผลิตภัณฑ์ข้างต้นต้องเปิดใช้งานซอฟต์แวร์ Cisco IOS XE for WLCs และมีการเปิดใช้งาน Out-of-Band AP Image Download feature enabled	ปิดการใช้งาน Out-of-Band AP Image Download feature จนกว่าจะสามารถ upgrade เป็น fixed software ตามที่ Cisco แนะนำ
ระดับ High 16 รายการ ได้แก่ CVE-2025-20186, CVE-2025-20182, CVE-2025-20154, CVE-2025-20162, CVE-2025-20192, CVE-2025-20164, CVE-2025-20122, CVE-2025-20210, CVE-2025-20202, CVE-2025-20191, CVE-2025-20197, CVE2025-20198, CVE-2025-20199, CVE-2025-20189, CVE-2025-20181 และ CVE-2025-20140		
ระดับ Medium 16 รายการ ได้แก่ CVE-2025-20193, CVE-2025-20194, CVE-2025-20195, CVE-2025-20187, CVE-2025-20190, CVE-2025-20213, CVE-2025-20157, CVE-2025-20155, CVE-2025-20223, CVE-2025-20221, CVE-2025-20196, CVE-2025-20137, CVE-2025-20216, CVE-2024-20475, CVE-2025-20214 และ CVE-2025-20151		

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 21 พ.ค. 2568
2) https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75279
3) https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-priviesc-WCk7bmmt
4) https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-api-nBPZcJCM