แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Cisco ออก Security Patch แก้ไขช่องโหว่ (CVE-2026-20127) ในผลิตภัณฑ์ Cisco Catalyst SD-WAN Controller และ Cisco Catalyst SD-WAN Manager

วันที่แจ้งเตือน 26 กุมภาพันธ์ 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Cisco ประกาศออก Security Patch เพื่อแก้ไขช่องโหว่ (CVE-2026-20127) ในผลิตภัณฑ์ Cisco Catalyst SD-WAN Controller และ Cisco Catalyst SD-WAN Manager (ชื่อเดิมคือ SD-WAN vSmart และ SD-WAN vManage) ที่ใช้บริหารจัดการเครือข่ายผ่านตัวควบคุมส่วนกลาง

ช่องโหว่ดังกล่าวเป็นลักษณะ Authentication Bypass จากความบกพร่องของกลไกการยืนยันตัวตน Peering Authentication Mechanism ซึ่งอาจเปิดโอกาสให้ผู้โจมตีสามารถใช้ช่องโหว่นี้เข้าสู่ Cisco Catalyst SD-WAN Controller ในฐานะ High-Privileged User เพื่อบริการจัดการเครือข่าย และปรับเปลี่ยนการตั้งค่า SD-WAN ซึ่งอาจทำให้เกิดความเสียหายต่อระบบและข้อมูลของหน่วยงานได้ นอกจากนี้ รายงานยังแจ้งว่าช่องโหว่ดังกล่าวอาจเชื่อมโยงกับช่องโหว่เดิม (CVE-2022-20775) ที่ผู้ไม่ประสงค์ดีใช้โจมตีตั้งแต่ปี 2023

เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานอุปกรณ์หรือระบบที่เกี่ยวข้อง พิจารณาดำเนินการอัปเดต Security Patch บน Cisco Catalyst SD-WAN Controller และ Cisco Catalyst SD-WAN Manager ที่ได้รับผลกระทบ (ทั้งในรูปแบบ On-Premises และ Cloud) ตามที่ผู้ผลิตให้คำแนะนำ รวมทั้ง ทบทวนการดำเนินการมาตรการ Cybersecurity ให้มีประสิทธิภาพอย่างสม่ำเสมอ

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

ข้อมูลอ้างอิง

1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
2. https://www.bleepingcomputer.com/news/security/critical-cisco-sd-wan-bug-exploited-in-zero-day-attacks-since-2023/
3. https://nvd.nist.gov/vuln/detail/CVE-2026-20127
4. https://nvd.nist.gov/vuln/detail/cve-2022-20775

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ