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 แก้ไขช่องโหว่ระดับวิกฤต 4 รายการ (CVE-2026-20184, CVE-2026-20147, CVE-2026-20180 และ CVE-2026-20186)

วันที่แจ้งเตือน 20 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cisco ออก Security Patch เพื่อแก้ไขช่องโหว่ความรุนแรงระดับวิกฤตจำนวน 4 รายการ ได้แก่

ช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ และ การแก้ไข	รายละเอียดช่องโหว่
CVE-2026-20184	Cisco Webex Services ที่เปิดใช้งาน Trust Anchors ในระบบ SSO ควรทำการอัปโหลดใบรับรอง SAML ของผู้ให้บริการระบุตัวตน (IdP) ฉบับใหม่ ไปยัง Control Hub	การตรวจสอบใบรับรองที่ไม่เหมาะสม (improper certificate validation) ในการเปิดใช้งาน single sign-on (SSO) เข้ากับ Control Hub ใน Webex Services ซึ่งอาจทำให้ผู้ไม่หวังดีสามารถปลอมตัวเป็นผู้ใช้ภายในและเข้าถึงบริการ Cisco Webex ได้
CVE-2026-20147	Cisco ISE or ISE-PIC Release earlier than 3.1 (Migrate to a fixed release) Cisco ISE Release 3.1 (3.1 Patch 11) Cisco ISE Release 3.2 (3.2 Patch 10) Cisco ISE Release 3.3 (3.3 Patch 11) Cisco ISE Release 3.4 (3.4 Patch 6) Cisco ISE Release 3.5 (3.5 Patch 3)	การตรวจสอบข้อมูลที่ผู้ใช้ส่งมาไม่เหมาะสม (insufficient validation of user-supplied input) ส่งผลให้ผู้ไม่หวังดีสามารถรันคำสั่งจากระยะไกล (Remote Code Execution) หรือทำการโจมตีแบบ Path Traversal บนอุปกรณ์ที่ได้รับผลกระทบได้
CVE-2026-20180 และ CVE-2026-20186	Cisco ISE Release earlier than 3.2 (Migrate to a fixed release) Cisco ISE Release 3.2 (3.2 Patch 8) Cisco ISE Release 3.3 (3.3 Patch 8) Cisco ISE Release 3.4 (3.4 Patch 4) Cisco ISE Release 3.5 (Not Vulnerable)	การตรวจสอบข้อมูลที่ผู้ใช้ส่งมา (user-supplied input) ไม่เหมาะสม ส่งผลให้ผู้ไม่หวังดีสามารถส่งคำขอ HTTP ที่สร้างขึ้นมาเป็นพิเศษไปยังอุปกรณ์ที่ได้รับผลกระทบ และ ผู้ไม่หวังดีได้รับสิทธิการเข้าถึงระดับผู้ใช้ (user-level access) บนระบบปฏิบัติการพื้นฐาน และสามารถยกระดับสิทธิเป็น root ได้

สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้งานอุปกรณ์หรือระบบที่เกี่ยวข้อง พิจารณาดำเนินการอัปเดต Security Patch เป็นเวอร์ชันล่าสุดตามคำแนะนำของผู้ผลิต

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

ข้อมูลอ้างอิง

1. https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL#vp
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-traversal-8bYndVrZ
4. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv#vp