แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Cisco และ SolarWinds ออก Security Patch แก้ไขช่องโหว่ในผลิตภัณฑ์

วันที่แจ้งเตือน 8 มิถุนายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cisco และ SolarWinds ได้ออก Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์ ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	• ช่องโหว่ CVE-2026-20230 เป็นช่องโหว่ แบบ Server-Side Request Forgery (SSRF) เกิดจากกระบวนการตรวจสอบข้อมูลนำเข้าใน HTTP request ของ Cisco Unified Communications Manager (Unified CM) และ Unified CM Session Management Edition ที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถส่งคำขอเพื่อหลอกให้เซิร์ฟเวอร์เขียนไฟล์ตามต้องการลงบนระบบปฏิบัติการ จากนั้นจะใช้เป็นฐานในการโจมตีในขั้นถัดไป เพื่อยกระดับสิทธิ์จากผู้ใช้งานทั่วไปไปเป็น Root เข้าควบคุมเซิร์ฟเวอร์ได้อย่างสมบูรณ์ • Cisco ได้ออก Security Patch แก้ไขสำหรับเวอร์ชัน 14 ให้อัพเดตเป็น 14SU6 และผู้ใช้งานเวอร์ชัน 15 จะต้องติดตั้ง Interim COP Patch ไปก่อน เนื่องจาก Service Update เต็มรูปแบบของเวอร์ชัน 15SU5 มีกำหนดเผยแพร่ในเดือนกันยายน 2026	ผลิตภัณฑ์ที่ได้รับผลกระทบ ได้แก่ Cisco Unified Communications Manager (Unified CM) เวอร์ชัน 14 และ 15
	• ช่องโหว่ CVE-2026-20245 เป็นช่องโหว่ประเภท Command Injection และ Privilege Escalation เกิดจากกระบวนการตรวจสอบข้อมูลนำเข้าจากผู้ใช้งานที่ไม่ถูกต้อง ผู้ไม่หวังดีจะใช้ช่องโหว่นี้เพื่ออัปโหลดไฟล์ที่ถูกสร้างขึ้นไปยังระบบที่ได้รับผลกระทบ จากนั้นจะใช้เทคนิค Command Injection ยกระดับสิทธิ์เป็นระดับ Root และเข้าควบคุมระบบได้ โดยช่องโหว่ดังกล่าวมีความเชื่อมโยงกับช่องโหว่ที่เคยถูกเปิดเผยก่อนหน้านี้ ได้แก่ CVE-2026-20182 และ CVE-2026-20127 เพื่อเข้าถึงระบบและดำเนินการโจมตีต่อเนื่อง • ปัจจุบัน Cisco ยังไม่มีการเผยแพร่แพตช์สำหรับแก้ไขช่องโหว่นี้ และยังไม่มีแนวทางลดความเสี่ยง (Workaround) ที่สามารถนำมาใช้ได้ในขณะนี้ จึงควรมีการติดตามการออก Patch แก้ไขช่องโหว่นี้ต่อไป	ส่งผลกระทบกับอุปกรณ์ Cisco Catalyst SD-WAN Manager ทั้งระบบที่ติดตั้งภายในองค์กร (On-Premises) บริการ Cisco SD-WAN Cloud-Pro ระบบ Cloud ที่ Cisco เป็นผู้ดูแล

ข้อมูลอ้างอิง Cisco

1. https://nvd.nist.gov/vuln/detail/CVE-2026-20230
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW
3. https://thehackernews.com/2026/06/cisco-patches-cve-2026-20230-in-unified.html
4. https://nvd.nist.gov/vuln/detail/CVE-2026-20245
5. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx
6. https://securityaffairs.com/193203/security/cisco-sd-wan-has-a-new-root-level-problem-and-theres-no-fix-yet.html

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Cisco และ SolarWinds ออก Security Patch แก้ไขช่องโหว่ในผลิตภัณฑ์

วันที่แจ้งเตือน 8 มิถุนายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
SolarWinds	• ช่องโหว่ CVE-2026-28318 เป็นช่องโหว่ประเภท Uncontrolled Resource Consumption เกิดจากการใช้ทรัพยากรของระบบมากเกินจำเป็น ทำให้ระบบทำงานช้าลงหรือหยุดให้บริการได้ (Denial-of-Service : DoS) ซึ่งผู้ไม่หวังดีจะส่งคำสั่ง HTTP POST ที่ถูกสร้างขึ้น เข้าสู่ระบบ เพื่อทำให้บริการ Serv-U หยุดทำงาน โดยไม่ต้องยืนยันตัวตน ด้วยการกำหนดค่า Content-Encoding: deflate ภายในคำขอที่ส่งเข้ามา โดยไม่ต้องอาศัยการกระทำใด ๆ จากผู้ใช้งานระบบ • SolarWinds ได้เผยแพร่ Serv-U เวอร์ชัน 15.5.4 Hotfix 1 เพื่อแก้ไขช่องโหว่ดังกล่าวแล้ว	ส่งผลกระทบกับระบบ SolarWinds Serv-U 15.5.4 และเวอร์ชันก่อนหน้า

ข้อมูลอ้างอิง SolarWinds

1. https://nvd.nist.gov/vuln/detail/CVE-2026-28318
2. https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28318
3. https://www.bleepingcomputer.com/news/security/cisa-hackers-now-exploit-solarwinds-serv-u-flaw-to-crash-servers/