

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

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



ช่องโหว่ในผลิตภัณฑ์ Cisco, VMware, Google Chrome และ Palo Alto หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 17 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Cisco, VMware, Google Chrome และ Palo Alto หลายรายการ เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	• ช่องโหว่ CVE-2026-76461 เป็นช่องโหว่ประเภท SQL Injection ส่งผลกระทบต่อซอฟต์แวร์ AsyncOS ในผลิตภัณฑ์ Cisco Secure Email Gateway ซึ่งเกิดจากการตรวจสอบข้อมูลในกระบวนการวิเคราะห์อีเมลไม่เพียงพอ ทำให้ผู้ไม่หวังดีสามารถโจมตีได้จากระยะไกลโดยไม่ต้องผ่านการยืนยันตัวตน และส่งอีเมลที่สร้างขึ้นและเรียกใช้คำสั่ง SQL เพื่อสั่งให้ระบบปฏิบัติการทำงานด้วยสิทธิ์ระดับ Root • Cisco แนะนำให้ผู้ใช้ผลิตภัณฑ์ ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามที่ระบุ	ส่งผลกระทบต่อผลิตภัณฑ์ Cisco Secure Email Gateway เวอร์ชัน • 15.5 และต่ำกว่า • 16.0 • 16.5

ข้อมูลอ้างอิง Cisco

- <https://nvd.nist.gov/vuln/detail/cve-2026-76461>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX>
- <https://www.cisa.gov/news-events/alerts/2026/09/14/cisa-adds-one-known-exploited-vulnerability-catalog>
- <https://thehackernews.com/2026/09/cisco-secure-email-gateway-flaw.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

ช่องโหว่ในผลิตภัณฑ์ Cisco, VMware, Google Chrome และ Palo Alto หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 17 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Broadcom	• ช่องโหว่ CVE-2026-59310 เป็นช่องโหว่ประเภท Directory Traversal ใน VMware vCenter Syslog Server โดยผู้ไม่หวังดีสามารถใช้ในการโจมตีได้โดยข้ามผ่านกระบวนการยืนยันตัวตน จากนั้นจะเรียกใช้โค้ดที่สร้างขึ้นเพื่อทำการโจมตีเพิ่มเติม และพบว่ามีผู้นำช่องโหว่ดังกล่าวไปใช้ในการโจมตีจริง • Broadcom แนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว ดำเนินการติดตั้ง Patch เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ • VMware Cloud Foundation 5.x, 9.0.x.x และ 9.1.x.x • VMware vSphere Foundation 9.0.x.x และ 9.1.x.x • VMware vCenter 9.0.x.x และ 9.1.x.x, 8.0 และ 7.0 • VMware Telco 3.0, 4.x, 5.0.x และ 5.1.x • VMware Telco Cloud Infrastructure 3.0

ข้อมูลอ้างอิง VMware

1. <https://nvd.nist.gov/vuln/detail/cve-2026-59310>
2. <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017>
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-59310
4. <https://www.bleepingcomputer.com/news/security/cisa-critical-vmware-vcenter-rce-flaw-now-exploited-by-ransomware-gangs/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT
Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

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

ช่องโหว่ในผลิตภัณฑ์ Cisco, VMware, Google Chrome และ Palo Alto หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 17 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Google	- ช่องโหว่ CVE-2026-91726 เป็นช่องโหว่ประเภท Out-of-Bounds Read ใน WebGL ซึ่งเกิดจากข้อผิดพลาดด้านการจัดการและความปลอดภัยของหน่วยความจำใน WebGL ทำให้ผู้ไม่หวังดีสามารถสร้างเนื้อหาเว็บไซต์เพื่อให้ Browser ทำงานผิดปกติหรือหยุดให้บริการได้ และจากนั้นจะเรียกใช้โค้ดอันตรายเพื่อทำการโจมตีเพิ่มเติมได้ - แนะนำให้ผู้ใช้งาน Google Chrome ดำเนินการอัปเดตซอฟต์แวร์ตามที่ผู้ผลิตแนะนำเป็นเวอร์ชัน 153.0.8010.47/48 สำหรับ Windows/macOS และเวอร์ชัน 153.0.8010.47 สำหรับ Linux	ส่งผลกระทบต่อ Google Chrome เวอร์ชันที่ต่ำกว่า 153.0.8010.47

ข้อมูลอ้างอิง Google Chrome

- <https://nvd.nist.gov/vuln/detail/cve-2026-91726>
- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0541751186.html
- <https://cyberpress.org/google-chrome-153-fixes-42-security-flaws/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT
Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

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

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



ช่องโหว่ในผลิตภัณฑ์ Cisco, VMware, Google Chrome และ Palo Alto หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 17 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Palo Alto	- ช่องโหว่ CVE-2026-0310 เป็นช่องโหว่ประเภท Buffer Overflow ในฟังก์ชันการประมวลผล XML ของซอฟต์แวร์ PAN-OS ทำให้ผู้ไม่หวังดีสามารถโจมตีได้จากระยะไกลโดยข้ามผ่านกระบวนการยืนยันตัวตน และสามารถเรียกใช้โค้ดอันตรายหรือคำสั่งที่สร้างขึ้นด้วยสิทธิ์ระดับ Root - Palo Alto แนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามที่ระบุ	ส่งผลกระทบต่อผลิตภัณฑ์ - Cloud NGFW ทุกเวอร์ชัน - PAN-OS เวอร์ชัน - 12.2.3 และต่ำกว่า - 12.1.4-h10 และต่ำกว่า - 11.2.4-h21 และต่ำกว่า - 11.1.4-h36 และต่ำกว่า - 10.2.7-h37 และต่ำกว่า - Prisma Access เวอร์ชัน - 11.2.4-h21 และต่ำกว่า - 10.2.7-h37 และต่ำกว่า

ข้อมูลอ้างอิง Palo Alto

- <https://nvd.nist.gov/vuln/detail/cve-2026-0310>
- <https://security.paloaltonetworks.com/CVE-2026-0310>
- <https://cybersecuritynews.com/palo-alto-pan-os-vulnerability-code-execution/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

