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 Google Chrome, Cisco, Linux Kernel และ Veeam หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 2 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Google Chrome, Cisco, Linux Kernel และ Veeam หลายรายการ เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Google	• **ช่องโหว่ CVE-2026-118306** ในเว็บบราวเซอร์ Google Chrome ซึ่งเป็นช่องโหว่ประเภท Memory Corruption ในการทำงานของ FileSystem ส่งผลให้ผู้ไม่หวังดีสามารถสร้างหน้าเว็บ HTML เพื่อทำการโจมตีผ่านช่องโหว่ดังกล่าว และสามารถนำไปสู่การรันโค้ดอันตรายจากระยะไกล (Remote Code Execution) ได้	ส่งผลกระทบต่อ Google Chrome เวอร์ชันที่ต่ำกว่า 156.0.8078.73 **คำแนะนำ** • แนะนำให้ผู้ใช้งาน ดำเนินการอัปเดตซอฟต์แวร์ตามที่ผู้ผลิตแนะนำเป็นเวอร์ชัน 156.0.8078.73/.74 สำหรับ Windows/MacOS และเวอร์ชัน 156.0.8078.73 สำหรับ Linux
Cisco	• **ช่องโหว่ CVE-2026-76418** ในผลิตภัณฑ์ Cisco Secure Firewall Adaptive Security Appliance (ASA) และ Cisco Threat Defense (FTD) เป็นช่องโหว่ประเภท Denial-of-Service เกิดจากข้อผิดพลาดในตรรกะการทำงาน (Logic Error) เมื่อมีการตั้งค่า webvpn และเปิด SSL VPN อย่างน้อยหนึ่ง interface บนอุปกรณ์ที่ต้องใช้ ASA หรือ FTD ส่งผลให้ผู้ไม่หวังดีสามารถใช้ช่องโหว่ดังกล่าว ส่งคำสั่งจากระยะไกลโจมตีอุปกรณ์ Cisco Secure Firewall ทำให้อุปกรณ์ reboot หรือบริการหยุดชะงัก	ส่งผลกระทบต่อผลิตภัณฑ์ • Cisco ASA9.16 และเวอร์ชันที่ต่ำกว่า, 9.18, 9.20, 9.22, 9.23 และ 9.24 • Cisco FTD 7.0 และเวอร์ชันที่ต่ำกว่า, 7.2, 7.4, 7.6, 7.7, 10.0 และ 10.1 **คำแนะนำ** • ควรดำเนินการอัปเกรดซอฟต์แวร์ Cisco ASA และ FDA เป็นเวอร์ชันที่ได้รับการแก้ไขแล้ว • ตรวจสอบอุปกรณ์ที่เปิดให้บริการ SSL VPN และมีเงื่อนไขการตั้งค่าตามที่ Cisco ระบุ

ข้อมูลอ้างอิง Google Chrome

1. https://nvd.nist.gov/vuln/detail/cve-2026-118306
2. https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_0562499947.html
3. https://www.securityweek.com/chrome-and-firefox-updates-patch-over-200-vulnerabilities

ข้อมูลอ้างอิง Cisco

1. https://nvd.nist.gov/vuln/detail/cve-2026-76418
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75
3. https://thehackernews.com/2026/10/cisco-patches-actively-exploited-asa.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 Google Chrome, Cisco, Linux Kernel และ Veeam หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 2 พฤศจิกายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Linux	• **ช่องโหว่ CVE-2026-98432** เป็นช่องโหว่ประเภท Use-After-Free ในส่วนของโค้ดเครือข่าย IPv4 TCP ของ Linux Kernel เกิดจาก Race Condition ระหว่างการจัดการคำขอเชื่อมต่อ TCP ซึ่งอาจทำให้ Kernel เข้าถึงข้อมูลในหน่วยความจำที่ถูกปล่อยคืนไปแล้ว ทำให้ผู้ไม่หวังดีสามารถส่งคำสั่งควบคุมจากระยะไกล (RCE) ด้วยสิทธิ Root ได้โดยไม่ต้องผ่านขั้นตอนการยืนยันตัวตน	ส่งผลกระทบต่อ Linux Kernel ตั้งแต่เวอร์ชัน 4.4 ในหลาย distribution • Ubuntu ,Red Hat • Amazon Linux • Oracle Linux • Debian, SUSE Linux **คำแนะนำ** • ผู้ดูแลระบบควรตรวจสอบความปลอดภัยและติดตั้ง Kernal Package ที่ได้รับการแก้ไขแล้ว • ควรจำกัดการเข้าถึงเฉพาะเครือข่ายหรือ IP Address ที่เชื่อถือได้ และพิจารณาบล็อก IPv4 TCP Packet ด้วย Firewall ตามคำแนะนำของผู้ผลิต
Veeam	• **ช่องโหว่ CVE-2026-108142** ในผลิตภัณฑ์ Veeam Backup & Replication ซึ่งเป็นช่องโหว่ประเภท Authorization Bypass เกิดจากกระบวนการตรวจสอบสิทธิบนบริการ CDP Coordinator Service ที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถข้ามขั้นตอนการตรวจสอบสิทธิ และทำการโจมตีเพิ่มเติมได้	ส่งผลกระทบต่อ ผลิตภัณฑ์ Veeam Backup & Replication • เวอร์ชัน 13.1.1.18 และก่อนหน้า • เวอร์ชัน 13.0.2.29 และก่อนหน้า ซอฟต์แวร์เวอร์ชันแก้ไข • 13.1.2 (Build 13.1.2.57) • 13.0.3 (Build 13.0.3.63)

ข้อมูลอ้างอิง Linux

1. https://nvd.nist.gov/vuln/detail/cve-2026-98432
2. https://git.kernel.org/pub/scm/linux/security/vulns.git/plain/cve/published/2026/CVE-2026-98432.mbox
3. https://www.bleepingcomputer.com/news/security/critical-linux-kernel-flaw-allows-remote-root-attacks-on-mptcp-servers/

ข้อมูลอ้างอิง Veeam

1. https://nvd.nist.gov/vuln/detail/cve-2026-108142
2. https://www.veeam.com/kb4948
3. https://cybersecuritynews.com/veeam-patches-authorization-bypass-vulnerability