

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

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



ช่องโหว่ในผลิตภัณฑ์ Microsoft, Cisco, Google Chrome และ Palo Alto เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 15 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

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

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	- ช่องโหว่ CVE-2026-96951 เป็นช่องโหว่ประเภท Command Injection ใน Windows Shell ทำให้ผู้ไม่หวังดีหลบเลี่ยงกลไกการรักษาความปลอดภัยของ Mark of the Web (MotW) จากนั้นทำการโจมตีเพิ่มเติมได้ - ช่องโหว่ CVE-2026-102866 เป็นช่องโหว่ใน Microsoft SharePoint Server เกิดจากการตรวจสอบ Cryptographic Signature ที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีหลบเลี่ยงขั้นตอนการยืนยันตัวตน สามารถยกระดับสิทธิ์ผ่านเครือข่ายและเข้าถึงข้อมูลสำคัญได้ - ช่องโหว่ CVE-2026-65674 เป็นช่องโหว่ประเภท Remote Code Execute ใน Microsoft SQL Server เกิดจากการนำข้อมูลที่ไม่น่าเชื่อถือเข้าสู่กระบวนการ Deserialization ทำให้ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนเรียกใช้โค้ดที่สร้างขึ้นเพื่อทำการโจมตีเพิ่มเติมได้ - Microsoft แนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว ดำเนินการอัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	- ช่องโหว่ CVE-2026-96951 ส่งผลกระทบต่อ Windows 10, Windows 11, Windows Sever 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022 และ Windows Server 2025 - ช่องโหว่ CVE-2026-102866 ส่งผลกระทบต่อ Microsoft SharePoint Server Subscription เวอร์ชัน 16.0.20326.20190 และต่ำกว่า - ช่องโหว่ CVE-2026-65674 ส่งผลกระทบต่อ Microsoft SQL Server 2019, Microsoft SQL Server 2022 และ Microsoft SQL Server 2025

ข้อมูลอ้างอิง Microsoft

- <https://nvd.nist.gov/vuln/detail/cve-2026-96951>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951>
- <https://nvd.nist.gov/vuln/detail/cve-2026-102866>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-102866>
- <https://nvd.nist.gov/vuln/detail/cve-2026-65674>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65674>
- <https://securityaffairs.com/200953/security/microsoft-patch-tuesday-sets-new-record-with-1415-cves-in-october-2026-updates.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 Microsoft, Cisco, Google Chrome และ Palo Alto เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 15 ตุลาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	• ช่องโหว่ CVE-2026-76519 เป็นช่องโหว่ประเภท Relative Path Traversal ในพีเจอาร์ Advanced Malware Protection (AMP) ของ Cisco Secure Email Gateway (SEG) เกิดจากการจัดการไฟล์แนบในอีเมลที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีใช้ช่องโหว่นี้ส่งอีเมลและไฟล์ที่สร้างขึ้นเพื่อโจมตีผ่านอุปกรณ์ที่ยังไม่ได้ติดตั้งแพตช์แก้ไข จากนั้นเรียกใช้คำสั่งด้วยสิทธิ์ระดับ Root เพื่อทำการโจมตีเพิ่มเติมได้ • Cisco แนะนำให้ผู้ใช้ผลิตภัณฑ์ ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามทีระบุ	ส่งผลกระทบต่อผลิตภัณฑ์ Cisco AsyncOS สำหรับ Cisco Secure Email Gateway เวอร์ชัน 15.5, 16.0 และ 16.5

ข้อมูลอ้างอิง Cisco

- <https://nvd.nist.gov/vuln/detail/cve-2026-76519>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkixp>
- <https://thehackernews.com/2026/10/cisco-warns-of-active-attacks.html>

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 Microsoft, Cisco, Google Chrome และ Palo Alto เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 15 ตุลาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Google	- ช่องโหว่ CVE-2026-110152 เป็นช่องโหว่ประเภท Buffer Overflow ใน ANGLE ซึ่งเป็นชั้นซอฟต์แวร์ของ Chrome ที่ทำหน้าที่แปลงคำสั่งด้านกราฟิก เกิดขึ้นเมื่อซอฟต์แวร์เขียนข้อมูลเกินพื้นที่หน่วยความจำที่จัดสรรไว้ ทำให้หน่วยความจำเสียหาย และผู้ไม่หวังดีอาจทำการโจมตีโดยการเปลี่ยนแปลงการทำงานของโปรแกรมหรือเรียกใช้โค้ดอันตรายที่สร้างขึ้นได้ - แนะนำให้ผู้ใช้งาน Google Chrome ดำเนินการอัปเดตซอฟต์แวร์ตามที่ผู้ผลิตแนะนำเป็นเวอร์ชัน 155.0.8059.79/.80 สำหรับ Windows/macOS และเวอร์ชัน 155.0.8059.79 สำหรับ Linux	ส่งผลกระทบต่อ Google Chrome เวอร์ชันที่ต่ำกว่า 155.0.8059.80

ข้อมูลอ้างอิง Google Chrome

- <https://nvd.nist.gov/vuln/detail/cve-2026-110152>
- https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_01668083673.html
- <https://cybersecuritynews.com/multiple-google-chrome-vulnerabilities/amp/>

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 Microsoft, Cisco, Google Chrome และ Palo Alto เสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 15 ตุลาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Palo Alto Network	- ช่องโหว่ CVE-2026-0322 โดยส่งผลกระทบต่อ Management Interface ของ PAN-OS ซึ่งผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนและสามารถเข้าถึงระบบผ่านเครือข่ายได้ จากนั้นจะเรียกใช้โค้ดหรือคำสั่งด้วยสิทธิ์ระดับ Root เพื่อทำการโจมตีเพิ่มเติมได้ และพบว่าช่องโหว่ดังกล่าวถูกนำไปใช้ในการโจมตีจริง - Palo Alto แนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามที่ระบุ	ส่งผลกระทบต่อผลิตภัณฑ์ PAN-OS เวอร์ชัน - 12.2.4 และต่ำกว่า - 12.1.10-h2 และต่ำกว่า - 11.2.16 และต่ำกว่า - 11.1.16-h3 และต่ำกว่า - 10.2.18-h12 และต่ำกว่า

ข้อมูลอ้างอิง Palo Alto

- <https://nvd.nist.gov/vuln/detail/cve-2026-0322>
- <https://security.paloaltonetworks.com/CVE-2026-0322>
- <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-rce-flaw-exploited-in-attacks/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT
Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์