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, PaloAlto และ Fortinet ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 17 มิถุนายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cisco, PaloAlto และ Fortinet ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	• ช่องโหว่ **CVE-2026-20262** ในผลิตภัณฑ์ Cisco Catalyst SD-WAN Manager ซึ่งถูกใช้โจมตีจริง เป็นช่องโหว่ประเภท Arbitrary File Write ที่มีการตรวจสอบ input ที่ส่งเข้ามาไม่เพียงพอเมื่อมีการ Upload ไฟล์ ทำให้ผู้ไม่หวังดีใช้ประโยชน์โดยส่ง HTTP request ที่ถูกสร้างขึ้นไปยัง API Endpoint เป้าหมาย จากนั้นจะสร้างหรือแก้ไขไฟล์สำคัญภายในระบบและอาจถูกนำไปใช้ในการยกระดับสิทธิ (Privilege Escalation) เพื่อเข้าถึงสิทธิระดับ Root บนระบบปฏิบัติการเพื่อดำเนินการโจมตีอื่นในภายหลัง • CISCO แนะนำให้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ Cisco Catalyst SD-WAN Manager ได้แก่ เวอร์ชัน 20.9.9.1 (และก่อนหน้า) 20.12.7.1 (และก่อนหน้า) 20.15.4.4 (และก่อนหน้า) 20.15.5.2 (และก่อนหน้า) 20.18.3 และ 20.1.1.1 (และก่อนหน้า)
PaloAlto	• ช่องโหว่ **CVE-2026-0257** ในผลิตภัณฑ์ GlobalProtect Portal ซึ่งถูกใช้โจมตีจริง เป็นช่องโหว่ประเภท Authentication Bypass ในส่วนของ Portal และ Gateway ของ PAN-OS ซึ่งเป็นส่วนสำคัญของระบบ GlobalProtect VPN ผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่นี้เพื่อหลบหลีกการรักษาและควบคุมความปลอดภัยภายในระบบ และทำการเชื่อมต่อ VPN เข้าสู่ระบบได้โดยไม่ต้องยืนยันตัวตน เพื่อควบคุมระบบขององค์กรได้ • PaloAlto แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่ออุปกรณ์ GlobalProtect Portal PAN-OS เวอร์ชัน 10.2, 11.1, 11.2, 12.1 และผลิตภัณฑ์ Prisma Access เวอร์ชัน 10.2.0 และ 11.2.0

ข้อมูลอ้างอิง Cisco

1. https://nvd.nist.gov/vuln/detail/CVE-2026-20262
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ
3. https://www.securityweek.com/cisco-patches-another-sd-wan-zero-day-exploited-in-attacks/

ข้อมูลอ้างอิง PaloAlto

1. https://nvd.nist.gov/vuln/detail/CVE-2026-0257
2. https://security.paloaltonetworks.com/CVE-2026-0257
3. https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/

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, PaloAlto และ Fortinet ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ

วันที่แจ้งเตือน 17 มิถุนายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Fortinet	• ช่องโหว่ **CVE-2026-39813** ในส่วนของ JRPC API ของ FortiSandbox ซึ่งถูกใช้โจมตีจริง เป็นช่องโหว่ประเภท Path Traversal ซึ่งผู้ไม่หวังดีสามารถข้ามการยืนยันตัวตนและส่ง HTTP request ที่สร้างขึ้นเพื่อหลบเลี่ยงการตรวจสอบสิทธิของระบบได้ • Fortinet แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ FortiSandbox เวอร์ชัน 4.4.0 - 4.4.8 และ 5.0.0 - 5.0.5
	• ช่องโหว่ **CVE-2026-39808 และ CVE-2026-25089** ในผลิตภัณฑ์ FortiSandbox เป็นช่องโหว่ประเภท OS Command Injection โดยมีรูปแบบการโจมตีคล้ายกับช่องโหว่ CVE-2026-39813 ซึ่งผู้ไม่หวังดีสามารถส่ง HTTP Request ที่ถูกสร้างขึ้น เพื่อสั่งรันโค้ดบนระบบเป้าหมายได้ โดยไม่ต้องยืนยันตัวตนและโจมตีระบบได้ • Fortinet แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ FortiSandbox เวอร์ชัน 4.4.0 - 4.4.8 FortiSandbox Cloud เวอร์ชัน 5.0.4 - 5.0.5 และ FortiSandBox PaaS เวอร์ชัน 5.0.4 - 5.0.5

ข้อมูลอ้างอิง Fortinet

1. https://nvd.nist.gov/vuln/detail/CVE-2026-39813
2. https://fortiguard.fortinet.com/psirt/FG-IR-26-112
3. https://nvd.nist.gov/vuln/detail/CVE-2026-39808
4. https://fortiguard.fortinet.com/psirt/FG-IR-26-100
5. https://nvd.nist.gov/vuln/detail/CVE-2026-25089
6. https://www.fortiguard.com/psirt/FG-IR-26-141
7. https://securityaffairs.com/193709/ai/fortinet-warned-as-three-critical-fortisandbox-bugs-come-under-attack.html