

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

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



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ในผลิตภัณฑ์ Cisco, Fortinet และ Check Point หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 16 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Cisco, Fortinet และ Check Point หลายรายการ เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	• ช่องโหว่ CVE-2026-20079 เป็นช่องโหว่ประเภท Authentication Bypass ในผลิตภัณฑ์ Cisco Secure Firewall Management Center (FMC) เกิดจากกระบวนการของระบบที่ถูกสร้างขึ้นโดยไม่ถูกต้องในช่วงการเริ่มต้นทำงานของอุปกรณ์ ทำให้ผู้ไม่หวังดีสามารถโจมตีจากระยะไกลโดยข้ามขั้นตอนการยืนยันตัวตน จากนั้นส่งคำร้อง HTTP ที่ถูกสร้างขึ้นและเรียกใช้สคริปต์บนระบบ และยกระดับสิทธิ์เป็น root ในระบบปฏิบัติการของอุปกรณ์ได้ • ช่องโหว่ CVE-2026-20316 เป็นช่องโหว่ประเภท Static Credential เกิดขึ้นในส่วนติดต่อผ่านเว็บของ FMC มีความเกี่ยวข้องกับการมีข้อมูลประจำตัวแบบคงที่ในระบบ ทำให้ผู้ไม่หวังดีที่ไม่ผ่านการยืนยันตัวตนสามารถเข้าสู่ระบบได้โดยใช้บัญชีที่มีสิทธิ์ระดับต่ำ และช่องโหว่นี้สามารถนำไปใช้โจมตีร่วมกับช่องโหว่อื่นของ FMC เพื่อยกระดับสิทธิ์ให้สูงขึ้น เพื่อใช้ในการเข้าถึงระบบได้ • Cisco แนะนำให้ผู้ผู้ใช้ผลิตภัณฑ์ ดำเนินการติดตั้ง Hotfix เวอร์ชันล่าสุด และจะเผยแพร่ซอฟต์แวร์รุ่นที่มีการ Hardening เพิ่มเติมต่อไป	ส่งผลกระทบต่อ ผลิตภัณฑ์ Cisco FMC เวอร์ชัน 7.0, 7.2, 7.4, 7.6, 7.7 และ 10.0

ข้อมูลอ้างอิง Cisco

- <https://nvd.nist.gov/vuln/detail/cve-2026-20079>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5Jp45V2>
- <https://nvd.nist.gov/vuln/detail/cve-2026-20316>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh>
- <https://thehackernews.com/2026/09/cisco-fmc-flaws-exploited-to-steal.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, Fortinet และ Check Point หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 16 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Fortinet	• ช่องโหว่ CVE-2025-25249 เป็นช่องโหว่ประเภท Heap-based Buffer Overflow ในระบบ FortiOS และ FortiSwitchManager ทำให้ผู้ไม่หวังดีสามารถโจมตีได้จากระยะไกลโดยไม่ต้องผ่านการยืนยันตัวตน จากนั้นส่งคำสั่งที่สร้างขึ้นเพื่อสั่งการให้ระบบเป้าหมายรันโค้ดหรือคำสั่งที่เป็นอันตรายได้ • Fortinet แนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว อัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อ ผลิตภัณฑ์ - Forti OS เวอร์ชัน 7.6.3 และต่ำกว่า - Forti OS เวอร์ชัน 7.4.8 และต่ำกว่า - Forti OS เวอร์ชัน 7.2.11 และต่ำกว่า - Forti OS เวอร์ชัน 7.0.17 และต่ำกว่า - Forti OS เวอร์ชัน 6.4 ทั้งหมด - FortiSwitchManager เวอร์ชัน 7.2.6 และต่ำกว่า - FortiSwitchManager เวอร์ชัน 7.0.5 และต่ำกว่า

ข้อมูลอ้างอิง Fortinet

1. <https://nvd.nist.gov/vuln/detail/cve-2025-25249>
2. <https://fortiguard.fortinet.com/psirt/FG-IR-25-084>
3. <https://socradar.io/blog/cve-2025-25249-pivotc2-fortigate-rat/>
4. <https://www.securityweek.com/fortinet-code-execution-flaw-exploited-in-pivotc2-rat-attacks/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



TCM-CERT
Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ช่องโหว่ในผลิตภัณฑ์ Cisco, Fortinet และ Check Point

หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 16 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Check Point	• ช่องโหว่ CVE-2026-85102 เป็นช่องโหว่ใน Check Point Quantum Security Gateway ที่เกิดจากการตรวจสอบข้อมูล Certificate ระหว่างกระบวนการเชื่อมต่อ VPN ที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถโจมตีได้จากระยะไกล โดยการเรียกใช้โค้ดที่สร้างขึ้นเพื่อสั่งการ Security Gateway ให้ทำงานตามที่ผู้ไม่หวังดีต้องการ • ช่องโหว่ CVE-2025-85103 เป็นช่องโหว่ประเภท Overflow ในผลิตภัณฑ์ Security Gateway, Security Management Server, Spark Firewall ที่เกิดขึ้นในตัวถอดรหัสใบรับรอง VPN ซึ่งใช้รูปแบบข้อมูล ASN.1 ทำให้ผู้ไม่หวังดีสามารถทำการโจมตีได้จากระยะไกล โดยการเรียกใช้งานโค้ดที่สร้างขึ้นเพื่อสั่งการ Security Gateway และ Security Management Server ให้ทำงาน • Check Point แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว อัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อ ผลิตภัณฑ์ Security Gateway และ Security Management Server เวอร์ชัน R81.20, R82, R82.10, R81.10.x และ R82.00.x รวมถึงเวอร์ชันที่ End on Support ได้แก่ R80 - R80.40, R81 และ R81.10

ข้อมูลอ้างอิง Check Point

1. <https://nvd.nist.gov/vuln/detail/cve-2026-85103>

2. <https://support.checkpoint.com/results/sk/sk1000118/>

3. <https://support.checkpoint.com/results/sk/sk1000117/>

4. <https://www.bleepingcomputer.com/news/security/dutch-ncsc-critical-check-point-vpn-flaws-exploitation-is-imminent/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ