

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, WatchGuard และ Apple หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 2 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

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

| ผู้ผลิต | รายละเอียดช่องโหว่                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | ผลิตภัณฑ์ที่ได้รับผลกระทบ                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Cisco   | <ul style="list-style-type: none"><li>• ช่องโหว่ CVE-2026-76504 เป็นช่องโหว่ประเภท Authentication Bypass ใน Cisco Catalyst SD-WAN Manager เกิดจากการจัดการ URI Encoding ใน HTTP Request ที่ไม่ถูกต้อง ส่งผลให้ผู้โจมตีสามารถส่ง HTTP Request ที่สร้างขึ้น ไปยัง API ของระบบที่ได้รับผลกระทบ จากนั้นหลีกเลี่ยงกระบวนการยืนยันตัวตน และเข้าถึง API โดยใช้สิทธิ์ระดับ Administrator ได้</li><li>• Cisco แนะนำให้ผู้ที่ใช้ผลิตภัณฑ์ ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามที่ระบุ</li></ul> | ส่งผลกระทบต่อผลิตภัณฑ์ Cisco Catalyst SD-WAN Manager เวอร์ชัน 20.9 และต่ำกว่า, เวอร์ชัน 20.12, 20.15, 20.18, 26.1 และ 26.2 |

### ข้อมูลอ้างอิง Cisco

- <https://nvd.nist.gov/vuln/detail/cve-2026-76504>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU>
- <https://www.securityweek.com/cisco-patches-exploited-catalyst-sd-wan-zero-day-vulnerability/>

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, Fortinet, WatchGuard และ Apple หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 2 ตุลาคม 2569

| ผู้ผลิต  | รายละเอียดช่องโหว่                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | ผลิตภัณฑ์ที่ได้รับผลกระทบ                                                                                                                                                                                                                   |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fortinet | <ul style="list-style-type: none"><li>• ช่องโหว่ CVE-2026-104286 เป็นช่องโหว่ประเภท Path Traversal ในเว็บอินเทอร์เฟซ (GUI) ของ Fortinet FortiMail ซึ่งมีการจำกัดเส้นทางไปยัง Directory ที่กำหนดไว้ ไม่ถูกต้อง รวมถึงการจัดการค่า Null Byte หรือ Null Character ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถหลีกเลี่ยงขั้นตอนการยืนยันตัวตน และทำการส่ง HTTP หรือ HTTPS Request ที่สร้างขึ้น เพื่อส่งเขียนไฟล์ลงในระบบของอุปกรณ์เป้าหมายได้</li><li>• Fortinet แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว ปฏิบัติตาม Workaround ที่ระบุไว้ จนกว่าจะพัฒนา Security Patch เพื่อแก้ไขช่องโหว่ดังกล่าวแล้วเสร็จ และเผยแพร่ต่อไป</li></ul> | ส่งผลกระทบต่อ ผลิตภัณฑ์ <ul style="list-style-type: none"><li>- FortiMail เวอร์ชัน 8.0.0 - 8.0.1</li><li>- FortiMail เวอร์ชัน 7.6.0 - 7.6.6</li><li>- FortiMail เวอร์ชัน 7.4.0 - 7.4.8</li><li>- FortiMail เวอร์ชัน 7.2.0 - 7.2.9</li></ul> |

### ข้อมูลอ้างอิง Fortinet

- <https://nvd.nist.gov/vuln/detail/cve-2026-104286>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>
- <https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/>

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, Fortinet, WatchGuard และ Apple หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 2 ตุลาคม 2569

| ผู้ผลิต    | รายละเอียดช่องโหว่                                                                                                                                                                                                                                                                                                                                                                                                                        | ผลิตภัณฑ์ที่ได้รับผลกระทบ                                                                                                                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WatchGuard | <ul style="list-style-type: none"><li>• ช่องโหว่ CVE-2026-86131 เป็นช่องโหว่ประเภท Code Injection ใน WatchGuard Firewall OS เกิดจากการประมวลผลการตั้งค่าของ BOVPN Over TLS Client ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถควบคุม VPN Server ฝั่งปลายทาง และสามารถส่งรับคำสั่งบนอุปกรณ์ Firebox ด้วยสิทธิ์ระดับ Root ได้</li><li>• WatchGuard แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว อัปเดตซอฟต์แวร์เป็นเวอร์ชันที่ได้รับการแก้ไขช่องโหว่แล้ว</li></ul> | <p>ส่งผลกระทบต่อ ผลิตภัณฑ์ WatchGuard</p> <ul style="list-style-type: none"><li>• Firewall OS 2026.3.2 และต่ำกว่า</li><li>• Firewall OS 2026.2.3 และต่ำกว่า</li><li>• Firewall OS 12.12.3 และต่ำกว่า</li><li>• Firewall OS 12.5.21 และต่ำกว่า</li></ul> |

### ข้อมูลอ้างอิง WatchGuard

1. <https://nvd.nist.gov/vuln/detail/cve-2026-86131>
2. <https://psirt.watchguard.com/CVE-2026-86131/>
3. <https://securityaffairs.com/200108/security/watchguard-fixes-critical-fireware-os-flaw-allowing-remote-code-execution.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ



**TCM-CERT**  
Thai Capital Market CERT



ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ  
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ผลกระทบต่อระบบ

☒ Loss of Confidentiality

☒ Loss of Integrity

☒ Loss of Availability

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

## ช่องโหว่ในผลิตภัณฑ์ Cisco, Fortinet, WatchGuard และ Apple หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 2 ตุลาคม 2569

| ผู้ผลิต | รายละเอียดช่องโหว่                                                                                                                                                                                                                                                                                                                                                                                    | ผลิตภัณฑ์ที่ได้รับผลกระทบ                                                                                                                                                                                                      |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apple   | <ul style="list-style-type: none"><li>ช่องโหว่ CVE-2026-86950 เป็นช่องโหว่ประเภท Out-of-Bounds Write ในส่วนของ CoreGraphics ของระบบปฏิบัติการ iOS, iPadOS และ macOS ส่งผลให้ผู้ไม่หวังดีสามารถเรียกใช้โค้ดที่สร้างขึ้น เพื่อเรียกใช้คำสั่งบนอุปกรณ์และทำการโจมตีเครื่องเป้าหมายเพิ่มเติมได้</li><li>Apple แนะนำให้ผู้ใช้งานผลิตภัณฑ์ดังกล่าว อัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว</li></ul> | <p>ส่งผลกระทบต่อ ผลิตภัณฑ์ Apple</p> <ul style="list-style-type: none"><li>iOS และ iPadOS เวอร์ชัน 26.7.1 และต่ำกว่า</li><li>macOS Sequoia เวอร์ชัน 15.8.1 และต่ำกว่า</li><li>macOS Tahoe เวอร์ชัน 26.7.1 และต่ำกว่า</li></ul> |

ข้อมูลอ้างอิง Apple

1. <https://nvd.nist.gov/vuln/detail/cve-2026-86950>
2. <https://thehackemews.com/2026/09/apple-patches-coregraphics-flaw.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ