แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Fortinet ออก Security Patch แก้ไขช่องโหว่จำนวน 4 รายการ (CVE-2026-22627, CVE-2026-24017, CVE-2025-54820 และ CVE-2026-24018)

วันที่แจ้งเตือน 20 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์กรณี Fortinet ได้ออกประกาศ security patch เพื่อแก้ไขช่องโหว่ความรุนแรงสูง 4 รายการ ดังนี้

ช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ	เวอร์ชั่นที่ได้รับผลกระทบ	รายละเอียดช่องโหว่ และ ผลกระทบ
CVE-2026-22627	FortiSwitchAXFixed	1.0.0 ถึง 1.0.1	ช่องโหว่การประมวลผล Link Layer Discovery Protocol (LLDP) ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีที่ไม่ได้รับการยืนยันตัวตนสามารถส่งแพ็กเก็ต LLDP ที่ถูกสร้างขึ้นเป็นพิเศษเพื่อสั่งให้ระบบประมวลผลคำสั่งที่ไม่ได้รับอนุญาตบนอุปกรณ์ได้
CVE-2026-24017	FortiWeb	8.0.0 ถึง 8.0.2 7.6.0 ถึง 7.6.5 7.4.0 ถึง 7.4.10 7.2.0 ถึง 7.2.11 7.0.0 ถึง 7.0.11	ช่องโหวประเภท Authentication Rate-Limit Bypass ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีที่ไม่ได้รับการยืนยันตัวตนสามารถหลีกเลี่ยงกลไกการจำกัดจำนวนความพยายามในการยืนยันตัวตนผ่านคำร้องที่ถูกสร้างขึ้นเป็นพิเศษ
CVE-2025-54820	FortiManager	7.4.0 ถึง 7.4.2 7.2.0 ถึง 7.2.10 6.4 ทุกเวอร์ชั่น	ช่องโหว่ประเภท Command Injection ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีไม่ได้รับการยืนยันตัวตนสามารถสั่งให้ระบบประมวลผลคำสั่งที่ไม่ได้รับอนุญาตผ่านคำร้องที่ถูกสร้างขึ้นเป็นพิเศษ หากบริการที่เกี่ยวข้องถูกเปิดใช้งาน
CVE-2026-24018	FortiClientLinux	7.4.0 ถึง 7.4.4 7.2.2 ถึง 7.2.12	ช่องโหว่ประเภท Privilege Escalation ซึ่งอาจเปิดโอกาสให้ผู้ใช้งานภายในระบบที่ไม่มีสิทธิระดับสูง (local unprivileged user) สามารถยกระดับสิทธิของตนเองเป็นระดับ root ได้

แนวทางการป้องกัน: ThaiCERT แนะนำให้ผู้ใช้งานและผู้ดูแลระบบพิจารณาดำเนินการดังต่อไปนี้

- อัปเดตผลิตภัณฑ์ Fortinet ที่ใช้งานให้เป็นเวอร์ชันล่าสุด
- ตรวจสอบและจำกัดสิทธิของบัญชีผู้ใช้งานในระบบ โดยเฉพาะบัญชีที่มีสิทธิระดับสูง
- จำกัดการเข้าถึงอุปกรณ์จากเครือข่ายภายนอก และอนุญาตเฉพาะแหล่งที่จำเป็นเท่านั้น
- เฝ้าระวังและตรวจสอบบันทึกเหตุการณ์ของระบบและอุปกรณ์เครือข่าย เพื่อค้นหาพฤติกรรมผิดปกติที่อาจเกี่ยวข้อง

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 19 มี.ค. 2569
2. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-024/