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

แจ้งเตือน Cisco และ Fortinet ออก Security Patch แก้ไขช่องโหว่ระดับร้ายแรง ในผลิตภัณฑ์ Cisco (CVE-2025-20265) และ Fortinet (CVE-2025-25256)

วันที่แจ้งเตือน 21 สิงหาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์พบว่า Cisco และ Fortinet ได้ออก Security Patch แก้ไขช่องโหว่ระดับร้ายแรง ดังนี้

(1) Cisco ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรง (CVE-2025-20265) ในระบบยืนยันตัวตนแบบ RADIUS ของซอฟต์แวร์ Secure Firewall Management Center (FMC) ซึ่งเป็นแพลตฟอร์มศูนย์กลางสำหรับบริหารจัดการไฟร์วอลล์ของ Cisco ผ่านเว็บหรือ SSH ซึ่งส่งผลกระทบต่อเวอร์ชัน FMC 7.0.7 และ 7.7.0 โดย Cisco ได้แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว ดำเนินการอัปเดต Security Patch เป็นเวอร์ชันที่ได้รับการแก้ไขแล้วทันที พร้อมทั้งตรวจสอบ Authentication/Access Logs และ System/Command Logs ของ FMC เพื่อหาพฤติกรรมที่ผิดปกติและพยายามเรียกใช้คำสั่งที่ไม่ได้รับอนุญาต และเฝ้าระวังเหตุ Privilege Escalation และการเปลี่ยนแปลงการตั้งค่านโยบายไฟร์วอลล์โดยมิชอบ

(2) Fortinet ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ระดับร้ายแรง (CVE-2025-25256) ในผลิตภัณฑ์ FortiSIEM โดยช่องโหว่นี้เป็น OS Command Injection (CWE-78) ที่ผู้โจมตีไม่ต้องยืนยันตัวตน และสามารถส่งคำสั่ง เพื่อให้ระบบประมวลผลโค้ดโดยไม่ได้รับอนุญาต ส่งผลกระทบต่อ FortiSIEM และมีคำแนะนำให้อัปเกรดเป็นเวอร์ชันที่ปิดช่องโหว่แล้วตามช่วงที่ผู้ผลิตระบุ ดังนี้

FortiSIEM เวอร์ชันที่ได้รับผลกระทบ	เวอร์ชันที่แนะนำให้อัปเกรด
5.4, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6 (ทุกเวอร์ชัน)	ย้ายไปยังเวอร์ชันที่สนับสนุนและได้รับแพตช์ (เช่น 7.4)
6.7.0 – 6.7.9	6.7.10 หรือสูงกว่า
7.0.0 – 7.0.3	7.0.4 หรือสูงกว่า
7.1.0 – 7.1.7	7.1.8 หรือสูงกว่า
7.2.0 – 7.2.5	7.2.6 หรือสูงกว่า
7.3.0 – 7.3.1	7.3.2 หรือสูงกว่า

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

ข้อมูลอ้างอิง

1. Cisco: https://www.bleepingcomputer.com/news/security/cisco-warns-of-max-severity-flaw-in-firewall-management-center/
2. Fortinet: https://thehackernews.com/2025/08/fortinet-warns-about-fortisiem.html

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ