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

Fortinet ออก Security Patch แก้ไขช่องโหว่ระดับร้ายแรง ในผลิตภัณฑ์ FortiSIEM (CVE-2025-64155)

วันที่แจ้งเตือน 15 มกราคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Fortinet ได้ประกาศเผยแพร่การอัปเดตซอฟต์แวร์เพื่อแก้ไขช่องโหว่ด้านความมั่นคงปลอดภัยระดับร้ายแรง (CVE-2025-64155) ในผลิตภัณฑ์ FortiSIEM

ช่องโหว่ดังกล่าวเป็นประเภท OS Command Injection ที่ผู้ไม่ประสงค์ดีอาจใช้ช่องโหว่ดังกล่าว เพื่อเรียกใช้โค้ดหรือคำสั่งที่ไม่ได้รับอนุญาตผ่านคำขอ TCP ที่สร้างขึ้นมา เข้าบุกรุกทำให้ระบบและข้อมูลของหน่วยงานได้รับความเสียหายได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่ใช้ผลิตภัณฑ์ FortiSIEM พิจารณาดำเนินการอัปเดตซอฟต์แวร์ เพื่อแก้ไขช่องโหว่ตามที่บริษัทผู้พัฒนาผลิตภัณฑ์แนะนำ และหากไม่สามารถดำเนินการได้ ควรพิจารณาดำเนินการเพื่อลดความเสี่ยง เช่น การจัดการการเข้าถึง TCP/UDP Port เป็นต้น รวมทั้งจัดให้มีการเฝ้าระวังพร้อมตรวจสอบบันทึกการใช้งาน (Logs) เพื่อให้สามารถตรวจพบและรับมือกับพฤติกรรมที่อาจบ่งชี้ถึงการใช้งานที่ผิดปกติได้อย่างทันท่วงที รวมถึงพิจารณาทบทวนมาตรการควบคุมด้านความมั่นคงปลอดภัยของระบบที่เปิดให้เข้าถึงจากภายนอกให้มีความเหมาะสมยิ่งขึ้น และติดตามประกาศด้านความมั่นคงปลอดภัยจากผู้พัฒนาผลิตภัณฑ์อย่างใกล้ชิด

Version	Affected	Solution
FortiSIEM Cloud	Not affected	Not Applicable
FortiSIEM 7.5	Not affected	Not Applicable
FortiSIEM 7.4	7.4.0	Upgrade to 7.4.1 or above
FortiSIEM 7.3	7.3.0 through 7.3.4	Upgrade to 7.3.5 or above
FortiSIEM 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiSIEM 7.1	7.1.0 through 7.1.8	Upgrade to 7.1.9 or above
FortiSIEM 7.0	7.0.0 through 7.0.4	Migrate to a fixed release
FortiSIEM 6.7	6.7.0 through 6.7.10	Migrate to a fixed release

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

ข้อมูลอ้างอิง

1. https://securityaffairs.com/186902/security/fortinet-fixed-two-critical-flaws-in-fortifone-and-fortisiem.html
2. https://nvd.nist.gov/vuln/detail/CVE-2025-64155
3. https://fortiguard.fortinet.com/psirt/FG-IR-25-772