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 ออกประกาศเตือนช่องโหว่ระดับร้ายแรง กระทบผลิตภัณฑ์หลายรายการ (CVE-2025-59718, CVE-2025-59719)

วันที่แจ้งเตือน 15 ธันวาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่าบริษัท Fortinet ได้ออกประกาศแจ้งเตือนช่องโหว่ระดับร้ายแรง 2 รายการ ได้แก่ CVE-2025-59718 และ CVE-2025-59719

ช่องโหว่ดังกล่าวมีสาเหตุจากความบกพร่องในการตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ (improper verification of cryptographic signature) ซึ่งผู้ไม่ประสงค์ดีใช้หลบเลี่ยงขั้นตอนพิสูจน์ตัวตน (Authentication Bypass) เข้าสู่ระบบผ่าน FortiCloud SSO และควบคุมอุปกรณ์ได้

- **CVE-2025-59718** ส่งผลกระทบต่อผลิตภัณฑ์ FortiOS, FortiProxy และ FortiSwitchManager ซึ่งระบบมีการตรวจสอบ SAML Response (Security Assertion Markup Language) ไม่ถูกต้อง เปิดช่องให้ผู้ไม่ประสงค์ดีสามารถใช้ SAML Message ที่ถูกปลอมแปลง เพื่อหลีกเลี่ยงขั้นตอนการยืนยันตัวตนของผู้ดูแลระบบ
- **CVE-2025-59719** ส่งผลกระทบต่อผลิตภัณฑ์ FortiWeb โดยพบว่าการตรวจสอบลายเซ็น SAML ยังไม่รัดกุมเพียงพอ ทำให้ผู้ไม่ประสงค์ดีสามารถปลอมแปลง SAML Response เพื่อเข้าสู่ระบบด้วยสิทธิ์ผู้ดูแลได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจที่มีการใช้งานผลิตภัณฑ์ Fortinet ที่เกี่ยวข้อง ดำเนินการตรวจสอบการเปิดใช้ฟังก์ชัน FortiCloud SSO ควรเร่งดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่ผู้ผลิตแนะนำ หากยังไม่สามารถดำเนินการอัปเดตได้ในทันที ให้พิจารณาปิดการใช้งาน FortiCloud SSO login เป็นการชั่วคราวควบคู่กับการเฝ้าระวังตรวจสอบบันทึกการทำงานของระบบ (Logs) และการตั้งค่ากลไกการพิสูจน์ตัวตนอย่างสม่ำเสมอ เพื่อค้นหาพฤติกรรมที่ผิดปกติ พร้อมทั้งทบทวนบัญชีผู้ดูแลระบบและกำหนดสิทธิ์การเข้าถึงให้สอดคล้องกับหลัก Least Privilege อย่างเคร่งครัด

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

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-forticloud-sso-login-auth-bypass-flaws/
2. https://fortiguard.fortinet.com/psirt/FG-IR-25-647
3. https://nvd.nist.gov/vuln/detail/CVE-2025-59718
4. https://nvd.nist.gov/vuln/detail/CVE-2025-59719

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ