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

แจ้งเตือนแคมเปญการโจมตีทางไซเบอร์ FortiBleed ใช้ข้อมูล Credential ที่รั่วไหล มุ่งเป้า Fortinet Firewall และ VPN

วันที่แจ้งเตือน 22 มิถุนายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีแคมเปญการโจมตีทางไซเบอร์ชื่อว่า FortiBleed โดยมีการใช้ข้อมูล Credential และสิทธิการเข้าถึงอุปกรณ์ Fortinet ที่เคยรั่วไหลในอดีตมาทำการทดสอบล็อกอินเข้าสู่ระบบ ซึ่งอาจทำให้ผู้โจมตีสามารถปลอมตัวเป็นผู้ดูแลระบบเพื่อเข้าถึงเครือข่ายภายในและส่งผลกระทบอย่างรุนแรงต่อความมั่นคงปลอดภัยของหลายองค์กรทั่วโลก รวมทั้ง **สำนักงานพบความพยายามใช้แคมเปญการโจมตีดังกล่าวต่อผู้ให้บริการของผู้ประกอบธุรกิจในตลาดทุนแล้ว** ซึ่งอาจส่งผลกระทบต่อความสามารถในการให้บริการได้ ดังนี้

การโจมตี	ผลิตภัณฑ์ที่ได้รับผลกระทบ
แคมเปญ FortiBleed พุ่งเป้าไปที่ FortiGate Firewall และ VPN ทั่วโลก โดยกลุ่มผู้ไม่หวังดีจะใช้ระบบอัตโนมัติสแกนหาอุปกรณ์ที่เชื่อมต่ออยู่บนอินเทอร์เน็ต และใช้วิธีการ Brute-force ระบบด้วย username/password เก่าผ่านทางหน้า Web Management Interface และอาจสามารถเข้าถึงและดาวน์โหลดไฟล์ Configuration จากอุปกรณ์ได้	• Fortinet FortiGate Firewall • Fortinet SSL VPN • ระบบบริหารจัดการ Fortinet ที่เปิดให้เข้าถึงจากอินเทอร์เน็ต • องค์กรที่ใช้รหัสผ่านซ้ำหรือไม่มีการเปิดใช้งาน MFA สำหรับบัญชีผู้ดูแลระบบและบัญชี VPN

คำแนะนำด้านความมั่นคงปลอดภัย

- ระงับการเข้าถึงหน้าต่างบริหารจัดการระบบ (Management Interface) จากเครือข่ายอินเทอร์เน็ตและจำกัดสิทธิการเชื่อมต่อเครือข่าย VPN เฉพาะกลุ่มที่อยู่ไอพี (IP Address) ภายในประเทศเท่านั้น พร้อมทั้งปิดกั้นการเชื่อมต่อจากต่างประเทศที่ไม่จำเป็น
- เปิดใช้งานระบบการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับผู้ดูแลระบบและผู้ใช้งาน VPN ทุกบัญชี
- เปลี่ยนรหัสผ่านของบัญชีผู้ดูแลระบบ Fortinet และบัญชี VPN ที่เกี่ยวข้องทั้งหมด โดยกำหนดให้มีความยาวและซับซ้อนตามมาตรฐานสากล และห้ามใช้รหัสผ่านซ้ำกับระบบอื่น
- บังคับรีเซ็ต Session และ Access Token ที่ยังใช้งานอยู่
- ตรวจสอบเครื่องของผู้ดูแลระบบว่ามีการติดมัลแวร์ประเภท Infostealer และดำเนินการแก้ไขที่เหมาะสม
- ตรวจสอบ Log การเข้าใช้งานย้อนหลัง เพื่อค้นหาการเข้าถึงจาก IP Address หรืออุปกรณ์ที่ไม่คุ้นเคย
- ตรวจสอบว่าระบบ Fortinet ได้รับการอัปเดตแพตช์ความปลอดภัยล่าสุดแล้วหรือไม่

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

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 22 มิ.ย. 2569
2. https://hackread.com/fortibleed-attack-fortinet-firewalls-credentials/?
3. https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure?

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ