แจ้งเตือน : ช่องโหว่

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน กรณี Console Chaos แคมเปญโจมตี Fortinet FortiGate Firewalls

วันที่แจ้งเตือน 18 มกราคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามข่าวสารด้านภัยคุกคามทางไซเบอร์ และได้รับการแจ้งเตือนเกี่ยวกับแคมเปญ Console Chaos เป็นการโจมตีที่มุ่งเป้าไปที่ Fortinet FortiGate Next-Generation Firewall (NGFW) ซึ่งเป็นส่วนติดต่อการจัดการของไฟร์วอลล์ ที่เปิดให้เข้าถึงได้จากอินเทอร์เน็ต ผู้ไม่ประสงค์ดีใช้เทคนิคปลอมแปลง IP Address และใช้ประโยชน์จากช่องโหว่ใน Web CLI (Command-Line Interface) เพื่อยกระดับสิทธิและเข้าควบคุมระบบ โดยพบว่าอุปกรณ์ที่ได้รับผลกระทบใช้เฟิร์มแวร์เวอร์ชัน 7.0.14 ถึง 7.0.16 ซึ่งเผยแพร่ระหว่างเดือนกุมภาพันธ์ถึงตุลาคม 2567

จากการวิเคราะห์ผลกระทบของภัยคุกคามแคมเปญ Console Chaos พบว่ามีความเสี่ยงสูงที่จะก่อให้เกิดความเสียหายต่อองค์กรในหลายระดับ โดยผู้ไม่ประสงค์ดีสามารถยกระดับสิทธิเพื่อเข้าควบคุมระบบไฟร์วอลล์ได้อย่างสมบูรณ์ ซึ่งเป็นจุดเริ่มต้นในการขยายขอบเขตการโจมตีไปยังระบบอื่น ๆ ภายในองค์กร ผู้ไม่ประสงค์ดีอาจสร้างบัญชีผู้ใช้งานที่มีสิทธิระดับสูง เพื่อหลบเลี่ยงการตรวจจับ ปรับเปลี่ยนการตั้งค่าความปลอดภัยตามต้องการ และสร้างช่องทาง VPN เพื่อเข้าถึงเครือข่ายภายในได้อย่างต่อเนื่อง ซึ่งการเข้าถึงในระดับนี้อาจนำไปสู่การโจรกรรมข้อมูลที่เป็นความลับ การหยุดชะงักของระบบงานสำคัญ หรือแม้กระทั่งการใช้เป็นฐานในการโจมตีองค์กรอื่น ๆ ต่อไป ส่งผลให้เกิดความเสียหายทั้งด้านการเงิน ชื่อเสียง และความเชื่อมั่นขององค์กรในระยะยาว

เพื่อรับมือกับภัยคุกคามแคมเปญ Console Chaos องค์กรจำเป็นต้องดำเนินมาตรการป้องกันและตอบสนองอย่างเป็นระบบและรวดเร็ว โดยเริ่มจากการปิดกั้นการเข้าถึงส่วนติดต่อการจัดการของไฟร์วอลล์จากอินเทอร์เน็ตโดยทันที พร้อมจำกัดการเข้าถึงให้เหลือเพียงเครือข่ายภายใน และ VPN ที่เชื่อถือได้เท่านั้น ควบคู่กับการปรับปรุงระบบด้วยการอัปเดตเฟิร์มแวร์ Fortinet FortiGate เป็นเวอร์ชันล่าสุด ทบทวนการตั้งค่าความปลอดภัยของระบบ นอกจากนี้ ต้องเพิ่มความเข้มงวดในการตรวจสอบและเฝ้าระวัง โดยเฉพาะการวิเคราะห์ Access logs ย้อนหลัง เพื่อตรวจหาร่องรอยการใช้งาน jsconsole จาก IP Address ที่น่าสงสัย เช่น 127.0.0.1 หรือ IP ของ Public DNS ที่อาจเชื่อมโยงกับการสร้างบัญชีผู้ใช้หรือการเปลี่ยนแปลงการตั้งค่า VPN โดยไม่ได้รับอนุญาต สำหรับกรณีที่ตรวจพบการบุกรุก องค์กรควรดำเนินการตอบสนองอย่างรวดเร็วด้วยการระงับและเปลี่ยนรหัสผ่านบัญชีผู้ใช้ทั้งหมด ตรวจสอบและกำจัดบัญชีผู้ใช้ที่ไม่ได้รับอนุญาต แก้ไขการตั้งค่า VPN ที่ถูกดัดแปลง พร้อมทั้งเก็บรวบรวมและวิเคราะห์หลักฐานที่เกี่ยวข้องเพื่อประเมินขอบเขตของความเสียหายที่เกิดขึ้นอย่างละเอียด

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

ข้อมูลอ้างอิง

1. https://arcticwolf.com/resources/blog-uk/campaign-targeting-publicly-exposed-management-interfaces-on-fortinet-fortigate-firewalls/
2. https://blog.netmanageit.com/console-chaos-a-campaign-targeting-publicly-exposed-management-interfaces-on-fortinet-fortigate-firewalls/