เอกสารการแจ้งเตือนกรณี Console Chaos: แคมเปญโจมตี Fortinet FortiGate Firewalls

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์กรณี Console Chaos: แคมเปญโจมตี Fortinet FortiGate Firewalls โดยแคมเปญ Console Chaos เป็นการโจมตีที่มุ่งเป้าไปที่ระบบ Fortinet FortiGate Next-Generation Firewall (NGFW) เพื่อใช้ประโยชน์จากช่องโหว่ใน Web CLI (Command-Line Interface) ของระบบเพื่อยกระดับสิทธิ์และเข้าถึงการจัดการไฟร์วอลล์ ซึ่งแคมเปญนี้มีเป้าหมายเพื่อเข้าควบคุมอุปกรณ์ ปรับเปลี่ยนการตั้งค่า และใช้เป็นทางผ่านในการเข้าถึงเครือข่ายอื่น ๆ[1]

จากรายงานของ Synacktiv ในปี 2566 ระบุว่า ช่องโหว่หมายเลข CVE-2022-26118 ได้เปิดโอกาสให้ผู้โจมตีสามารถใช้คำสั่ง newcli เพื่อสร้างผู้ใช้งาน backdoor โดยกำหนดค่า IP Address เป็น 127.0.0.1 (loopback) ซึ่งเป็นการปลอมแปลงว่าเป็นการส่งคำสั่งจาก Web CLI (jsconsole) ที่ถูกต้อง วิธีนี้ทำให้ผู้โจมตีสามารถเพิ่มสิทธิ์และเข้าควบคุมระบบได้โดยไม่ต้องยืนยันตัวตนแบบปกติ[2]

อุปกรณ์ที่ได้รับผลกระทบใช้เฟิร์มแวร์ระหว่างเวอร์ชัน 7.0.14 - 7.0.16 (ช่วงเดือนกุมภาพันธ์ - ตุลาคม 2567) ผู้ดูแลระบบควรอัปเดตเป็นเวอร์ชันล่าสุดและตรวจสอบความปลอดภัยอย่างสม่ำเสมอ เพื่อป้องกันการโจมตีประเภทนี้

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตี และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

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