ช่องโหว่ Kubernetes (CVE-2023-5528)

เหตุการณ์นี้ ที่ผู้โจมตีสามารถได้รับการเข้าถึงและดำเนินการคำสั่งระยะไกลด้วยสิทธิ์สูงสุด เกี่ยวข้องโดยตรงกับประเด็นหลักหลายข้อใน OWASP Top 10 2021:

- A01:2021 - Broken Access Control (การควบคุมการเข้าถึงที่ผิดพลาด): ผู้โจมตีที่ใช้ช่องโหว่นี้สามารถหลีกเลี่ยงการจำกัดการเข้าถึงเพื่อดำเนินการที่ไม่ได้รับอนุญาต.
- A03:2021 - Injection (การฉีดข้อมูล): วิธีการใช้ไฟล์ YAML ที่มีเจตนาไม่ดีบ่งชี้ถึงช่องโหว่แบบ injection ที่อนุญาตให้ผู้โจมตีส่งข้อมูลเสียหายไปยังตัวแปลงข้อมูล.
- A05:2021 - Security Misconfiguration (การกำหนดค่าความปลอดภัยที่ไม่ถูกต้อง): ช่องโหว่ดังกล่าวมักเกิดจากการกำหนดค่าเริ่มต้นที่ไม่ปลอดภัยหรือการตั้งค่าที่ไม่สมบูรณ์ ชี้ให้เห็นถึงปัญหาการกำหนดค่าที่ไม่ปลอดภัย.

กลุ่มอาชญากรไซเบอร์ RedCurl ใช้เครื่องมือของ Windows PCA

การใช้เครื่องมือ Windows ที่ถูกต้องตามกฎหมายเพื่อวัตถุประสงค์ที่เป็นอันตรายแสดงให้เห็นถึงเทคนิคการโจมตีที่ซับซ้อนซึ่งใช้ประโยชน์จาก:

- A04:2021 - Insecure Design (การออกแบบที่ไม่ปลอดภัย): การใช้ประโยชน์จากคุณลักษณะพื้นฐานของ Windows เพื่อวัตถุประสงค์ที่เป็นอันตรายชี้ให้เห็นถึงการขาดหลักการออกแบบที่ปลอดภัยซึ่งคาดการณ์และลดความเสี่ยงจากการใช้งานที่ไม่เหมาะสม.
- A07:2021 - Identification and Authentication Failures (การล้มเหลวในการระบุตัวตนและการตรวจสอบสิทธิ์): ความสามารถของผู้โจมตีในการดำเนินคำสั่งโดยไม่มีการตรวจสอบที่เหมาะสมแสดงถึงความล้มเหลวในการแยกแยะการกระทำของผู้ใช้ที่ถูกต้องกับผู้โจมตี.

สำหรับทั้งสองสถานการณ์ กลยุทธ์การบรรเทาปัญหาควรรวมถึงการตรวจสอบความปลอดภัยอย่างครบถ้วนและการอัปเดตระบบที่เกี่ยวข้อง โดยเน้นการกำหนดค่าที่ปลอดภัย, การควบคุมการเข้าถึงตามหลักการสิทธิ์น้อยที่สุด, กลไกการตรวจสอบสิทธิ์ที่แข็งแกร่ง, และการตรวจจับภัยคุกคามอย่างรวดเร็ว.

สำคัญสำหรับองค์กรในการอัปเดตการปฏิบัติการความปลอดภัยและระบบของตนเป็นประจำเพื่อป้องกันช่องโหว่เหล่านี้และให้แน่ใจว่าพวกเขาสอดคล้องกับมาตรฐานความปลอดภัยปัจจุบันเช่น OWASP Top 10.