แจ้งเตือน : ช่องโหว่

ระดับ : High

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☐ Non-Compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับสูง (High) ของระบบ Container Runtime Interface ที่ใช้มาตรฐาน OCI (CRI-O) สำหรับซอฟต์แวร์ Kubernetes ทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ (Privilege Escalation) (CVE-2022-0811)

วันที่แจ้งเตือน 21 มีนาคม 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนช่องโหว่ระดับสูง (High) ของระบบ Container Runtime Interface ที่ใช้มาตรฐาน OCI (CRI-O) สำหรับซอฟต์แวร์ Kubernetes ที่ทำให้สามารถ Bypass การป้องกันความมั่นคงปลอดภัยและตั้งค่า Parameter แปลกปลอมบน Kernel (Arbitrary Kernel Parameter) โดยช่องโหว่ข้างต้นทำให้ผู้ไม่หวังดีสามารถดำเนินการบนเครื่องปลายทางดังนี้

- มีสิทธิใช้งานกลุ่มของทรัพยากรที่ใช้งาน (Pod) บน Cluster ของซอฟต์แวร์ Kubernetes
- เข้าถึงเครื่องแม่ข่ายเพื่อทำการโจมตี Container โดยตรง (Container Escape)
- เรียกใช้คำสั่งแปลกปลอมโดยไม่ได้รับอนุญาต (Arbitrary Code Execution) ส่งผลให้สามารถการยกระดับสิทธิของระบบปฏิบัติการ (Local Privilege Escalation) เป็นสิทธิสูงสุด (Root) บน Cluster Node ได้

โดยเวอร์ชันระบบ Container Runtime (CRI-O) ที่ได้รับผลกระทบของช่องโหว่ข้างต้นได้แก่ 1) ตั้งแต่ 1.19.0 ถึงก่อน 1.19.6 2) ตั้งแต่ 1.20.0 ถึงก่อน 1.20.7 3) ตั้งแต่ 1.21.0 ถึงก่อน 1.21.6 4) ตั้งแต่ 1.22.0 ถึงก่อน 1.22.3 และ 5) ตั้งแต่ 1.23.0 ถึงก่อน 1.23.2

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการ ดังนี้

1. ตรวจสอบรายละเอียดของช่องโหว่ข้างต้นและพิจารณาดำเนินการอัปเดต Security Patch ให้เป็นเวอร์ชั่น 1.19.6, 1.20.7, 1.21.6, 1.22.3, 1.23.2, 1.24.0 ซึ่งสามารถศึกษารายละเอียดเพิ่มเติมตามรายละเอียดด้านล่าง

   - https://github.com/cri-o/cri-o/releases *External Link*

2. กรณีมีข้อจำกัดในการติดตั้ง Security Patch สามารถใช้วิธีการเพื่อที่จะลดความเสี่ยงเบื้องต้น (Workaround) จากช่องโหว่ข้างต้นโดยผู้ดูแลระบบดำเนินการได้ดังนี้

   1) ใช้คำสั่ง “**manage_ns_lifecycle**” **ตั้งค่าเป็น** “**false**” โดยคำสั่งนี้สามารถใช้ได้ในเวอร์ชัน 1.19 และ 1.20 เท่านั้น

   2) ตั้งค่าการปฏิเสธในการเข้าถึง Pod โดยตั้งค่าการใช้งาน “**sysctl**” **ตั้งค่าเป็น** “**+**”

   3) ตั้งค่าการรักษาความปลอดภัยใน Pod (Podsecuritypolicy) โดยตั้งค่าการใช้งาน “**sysctl**” **ทั้งหมดเป็น** “**forbidden**”

   หมายเหตุ: หากมีความจำเป็นในการใช้งาน SysCtl Interface เพื่อบริหารจัดการ Runtime Kernel Parameter อาจมีผลกระทบจากการปิดการใช้งาน SysCtl ตาม 2) และ 3) และไม่สามารถดำเนินการได้

   โดยสามารถศึกษารายละเอียดได้ตามรายละเอียดด้านล่าง

   - https://github.com/advisories/GHSA-6x2m-w449-qwx7 *External Link*

แจ้งเตือนช่องโหว่ระดับสูง (High) ของระบบ Container Runtime Interface ที่ใช้มาตรฐาน OCI (CRI-O) สำหรับซอฟต์แวร์ Kubernetes ทำให้ผู้ไม่ประสงค์ดีสามารถยกระดับสิทธิ์ (Privilege Escalation) (CVE-2022-0811)

วันที่แจ้งเตือน 21 มีนาคม 2565

3. ผู้ดูแลระบบควรประเมินความเสี่ยงจากวิธีการบรรเทาและลดความเสี่ยงและควรดำเนินการทดสอบการติดตั้ง Patch หรือการใช้โปรแกรม Workaround รวมถึงการตั้งค่าการป้องกันบนอุปกรณ์รักษาความปลอดภัย ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

ข้อมูลอ้างอิง

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0811
2. https://www.cisa.gov/uscert/ncas/current-activity/2022/03/18/cri-o-security-update-kubernetes
3. https://nvd.nist.gov/vuln/detail/CVE-2022-0811
4. https://access.redhat.com/security/cve/cve-2022-0811#cve-cvss-v3
5. https://www.geekinteger.com/cri-o-container-engine-bug-allows-kubernetes-container-escape/

External Link