แจ้งเตือน : ช่องโหว่

Critical

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 พบช่องโหว่ใน GitLab Community Edition และ Enterprise Edition

วันที่แจ้งเตือน 26 กันยายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

GitLab ออกอัปเดตเพื่อแก้ไขช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-45409 มีคะแนน (CVSSv3: 9.8) ส่งผลกระทบต่อการติดตั้งแบบ self-managed ของ GitLab Community Edition (CE) และ GitLab Enterprise Edition (EE) ช่องโหว่ดังกล่าวเกิดจาก input validation ทำให้เกิดความเสี่ยงที่ผู้โจมตีอาจเข้าถึงระบบ GitLab โดยไม่ต้องผ่านการยืนยันตัวตน และใช้สิทธิที่ได้รับเพื่อแก้ไขหรือลบข้อมูลสำคัญ รวมทั้งอาจเป็นจุดเริ่มต้นในการโจมตีระบบอื่น ๆ ที่เชื่อมโยงกับ GitLab ได้

ผลิตภัณฑ์ที่ได้รับผลกระทบ

- GitLab CE/EE เวอร์ชัน 16.11.10 และก่อนหน้า
- GitLab CE/EE เวอร์ชัน 17.0.8, 17.1.8, 17.2.7, 17.3.3 และก่อนหน้า

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจจะเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งเตือนผู้ประกอบธุรกิจที่มีการใช้งานระบบดังกล่าว ดำเนินการดาวน์โหลดและอัปเดตเป็นเวอร์ชันล่าสุดที่ได้รับการแก้ไขช่องโหว่ และจำกัดการเข้าถึงโดยใช้ไฟร์วอลล์หรือ access control lists เพื่อจำกัดการเข้าถึง GitLab จากภายนอก รวมทั้งติดตามข่าวสาร การอัปเดตความปลอดภัยใหม่ ๆ และตั้งค่าการแจ้งเตือนสำหรับกิจกรรมที่น่าสงสัยในระบบที่บริษัทท่านนำมาใช้เป็นประจำ เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-120
2) https://www.bleepingcomputer.com/news/security/gitlab-releases-fix-for-critical-saml-authentication-bypass-flaw/