TLP:CLEAR

เอกสารการแจ้งเตือนกรณีพบช่องโหว่ใน GitLab Community Edition และ Enterprise Edition

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณี พบช่องโหว่ใน GitLab Community Edition และ Enterprise Edition โดย GitLab ได้ออกอัปเดตเพื่อแก้ไขช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-45409 มีคะแนน (CVSSv3 : 9.8) ซึ่งส่งผลกระทบต่อการติดตั้งแบบ self-managed ของ GitLab Community Edition และ Enterprise Edition โดยที่ช่องโหว่ดังกล่าวเกิดจาก input validation ทำให้ผู้ไม่ประสงค์ดีสามารถหลีกเลี่ยงการยืนยันตัวตนผ่าน Security Assertion Markup Language (SAML) และเข้าถึง GitLab โดยการส่ง SAML responses ที่ปรับแต่งมาเป็นพิเศษ [1]

ช่องโหว่ส่งผลกระทบต่อผลิตภัณฑ์ดังต่อไปนี้:

- GitLab CE/EE เวอร์ชัน 16.11.10 และเก่ากว่า
- GitLab CE/EE เวอร์ชัน 17.0.8, 17.1.8, 17.2.7, 17.3.3 และเก่ากว่า [2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบ กิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

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/

TLP:CLEAR