แจ้งเตือน : ช่องโหว่

ระดับ : Critical

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

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☐ Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ระดับร้ายแรง (Critical) ที่ทำให้ผู้ไม่หวังดีเข้าควบคุมบัญชีผู้ใช้งานของโปรแกรม Gitlab (CVE-2022-1162)

วันที่แจ้งเตือน 7 เมษายน 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ระดับร้ายแรง (Critical) ที่ทำให้ผู้ไม่หวังดีเข้าควบคุมบัญชีผู้ใช้งานของโปรแกรม Gitlab (CVE-2022-1162) ซึ่งเป็นเครื่องมือบริการจัดการควบคุมเวอร์ชัน Source Code (Git Repository) และเครื่องมือจัดการ CI/CD (Continuous Integration and Continuous Delivery) โดยช่องโหว่เกิดจากกลไกการใช้รหัสผ่านแบบ Hardcode จากการใช้วิธีลงทะเบียนบัญชีผู้ใช้งานและการยืนยันตัวตนในรูปแบบ OmniAuth เช่น OAuth LDAP และ SAML เป็นต้น

ทั้งนี้โปรแกรม Gitlab ที่ได้รับผลกระทบได้แก่เวอร์ชันที่ 14.7 14.8 และ 14.9 ทั้งในรูปแบบ Community Edition (CE) และ Enterprise Edition (EE)

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบและพิจารณาดำเนินการอัปเดต Security Patch เวอร์ชัน 14.9.2 14.8.5 และ 14.7.7 เพื่อแก้ไขช่องโหว่โปรแกรม Gitlab ซึ่งสามารถรายละเอียดเพิ่มเติมได้ที่

- https://about.gitlab.com/releases/2022/03/31/critical-security-release-gitlab-14-9-2-released/ *External Link*

2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

1) https://nvd.nist.gov/vuln/detail/CVE-2022-1162
2) https://vuldb.com/?id.196480
3) https://gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1162.json
4) https://thehackernews.com/2022/04/gitlab-releases-patch-for-critical.html?fbclid=IwAR2TYbFpUE8ON5ou9m7Zqfte8QyOZFBdmquLPqJuEr7od3aHMoYj6mUanH4
5) https://www.bleepingcomputer.com/news/security/critical-gitlab-vulnerability-lets-attackers-take-over-accounts/?fbclid=IwAR3F0wNuEY5lLYJ96XM7BsMBQRYc8-LwuTqHuZOnJSGqtQdqbbVlUXvF-ek *External Link*