國立成功大學 National Cheng Kung University

(ANA事件單通知:TACERT-ANA-2025031811035959)(【漏洞預警】GitLab 的社群版(CE)及企業版(EE)存在2個重大資安漏洞)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025031811035959	發佈時間	2025-03-18 11:18:01
事故類型	ANA-漏洞預警	發現時間	2025-03-18 11:18:01
影響等級	中		

[主旨說明:]【漏洞預警】GitLab 的社群版(CE)及企業版(EE)存在2個重大資安漏洞

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202503-00000007

GitLab 是基於Git的整合軟體開發(DevSecOps)平台，提供版本控制、CI/CD自動化等功能。近期GitLab針對社群版(CE)及企業版(EE)發布多個資安漏洞公告並提供修補版本，其中以CVE-2025-25291(CVSS 4.x：8.8) 與CVE-2025-25292(CVSS 4.x：8.8)為重大資安漏洞，這二個繞過身分驗證漏洞存在ruby-saml的程式庫，攻擊者能存取已經過身分驗證且有效簽署的SAML檔，作為另一個有效使用者進行身分驗證。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

GitLab CE/EE

[建議措施:]

將 GitLab CE/EE 更新至 17.7.7、17.8.5、17.9.2(含)之後版本

[參考資料:]
1. GitLab 的社群版(CE)及企業版(EE)存在2個重大資安漏洞： https://www.twcert.org.tw/tw/cp-169-10016-550eb-1.html
2. GitLab Critical Patch Release: 17.9.2, 17.8.5, 17.7.7： https://about.gitlab.com/releases/2025/03/12/patch-release-gitlab-17-9-2-released/#guest-with-custom-admin-group-member-permissions-can-approve-the-users-invitation-despite-user-caps
3. CVE-2025-25291： https://nvd.nist.gov/vuln/detail/CVE-2025-25291
4. CVE-2025-25292： https://nvd.nist.gov/vuln/detail/CVE-2025-25292

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw