

教育機構 ANA 通報平台

|      |                             |      |                        |
|------|-----------------------------|------|------------------------|
| 發佈編號 | TACERT-ANA-2026102701102727 | 發佈時間 | 2026-10-27<br>13:42:28 |
| 事故類型 | ANA-漏洞預警                    | 發現時間 | 2026-10-27<br>13:42:28 |
| 影響等級 | 中                           |      |                        |

[主旨說明:] **【漏洞預警】GitLab 存在 2 項高風險安全漏洞(CVE-2026-97229 與 CVE-2026-110264)，請儘速確認並進行處置**

[內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-200-202610-00000022

研究人員發現 GitLab 社群版(CE)與企業版(EES)存在 2 項整數溢位(Integer Overflow)漏洞(CVE-2026-97229 與 CVE-2026-110264)。

**【CVE-2026-97229】** 前者於特定條件下，未經身分鑑別之遠端攻擊者可藉由於 CI/CD 組態中使用特製之正規表示式，進而於 GitLab 伺服器執行任意程式碼。

**【CVE-2026-110264】** 後者因編譯特製之正規表示式時發生整數溢位，於特定條件下，未經身分鑑別之遠端攻擊者可於 GitLab 伺服器執行任意程式碼，請儘速確認並進行處置。

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」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

GitLab CE/EE 7.0 至 18.11.13(不含)、19.0 至 19.0.10(不含)、19.1 至 19.1.9(不含)、19.2 至 19.2.9(不含)、19.3 至 19.3.6(不含)、19.4 至 19.4.3(不含)及 19.5 至 19.5.1(不含)版本

**[建議措施:]**

官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下：

<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/>

<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>

**[參考資料:]**

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-97229>
2. <https://nvd.nist.gov/vuln/detail/CVE-2026-110264>
3. <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/>
4. <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>