SupplyGuard

供應鏈健檢報告

程式庫 crater-invoice-inc/crater ｜ 掃描日期 2026 年 11 月 2 日 ｜ 檢查 631 個開源元件

這是範例報告。掃描對象是開源專案 Crater（給中小企業用的開源發票系統）在 2024 年 8 月的版本（commit 05d5ce2）。這個專案已約兩年沒有更新，風險會比持續維護的系統多，結果也不代表專案之後的版本。

有 7 個項目建議排入近期更新，有 3 個語言版本要請管伺服器的人確認。

0	7	3	58
立即處理	**排入近期更新**	**需要確認**	**跟著例行更新**
上線的元件已確認有人拿來攻擊，或套件被植入惡意程式	預測被利用的機率偏高，或已遭攻擊但只在建置時使用	要看伺服器實際版本才知道有沒有影響	被利用的機率較低，不用單獨處理

以上是項目數。同一個套件有多個漏洞時算一項，共 220 筆已知漏洞與確認項目。

重點項目

這幾項最值得先看。每一項都可以直接轉給工程或外包團隊。

vite 2.6.14 排入近期更新 僅建置用

這是什麼　JavaScript 前端開發工具框架，用於建置與開發網頁應用程式。

為什麼要注意　美國資安主管機關 CISA 已確認，這個漏洞有人實際拿來攻擊。攻擊者可能透過特定請求讀取原本不應對外公開的檔案內容，進而讓公司系統中的敏感資料外洩。這個套件只在開發或建置時用到，不會跟著系統上線執行，風險比上線的套件低。

怎麼處理　請工程或外包團隊先升級到 4.5.12 以上，可解決最要緊的漏洞，但這是跨 2 個大版本升級，可能要改程式，建議先排測試。要修掉全部 21 個漏洞，需要升級到 6.4.4 以上。

第一步指令：`npm install -D vite@4.5.12`

漏洞編號　CVE-2025-31125、CVE-2025-30208、CVE-2025-31486、CVE-2023-34092、CVE-2025-32395、CVE-2026-112942 等共 21 個

© 2026 DataAgent AI Lab

axios `0.19.2` 排入近期更新

這是什麼 一個用來在瀏覽器與 Node.js 中發送 HTTP 請求的套件。

為什麼要注意 依全球漏洞預測資料 EPSS，這個漏洞被利用的機率高於 96% 的已知漏洞。攻擊者可能讓本應被排除的內部位址請求仍經由代理送出，進而接觸到原本應限制存取的內部服務或資料。

怎麼處理 請工程或外包團隊先升級到 0.32.0 以上，可解決最要緊的漏洞，但這是跨大版本升級，可能要改程式，建議先排測試。要修掉全部 25 個漏洞，需要升級到 0.33.0 以上。

第一步指令：`npm install axios@0.32.0`

漏洞編號 CVE-2026-44492、CVE-2021-3749、CVE-2026-44496、CVE-2026-25639、CVE-2020-28168、CVE-2026-40175 等共 25 個

---

dompdf/dompdf `v1.2.2` 排入近期更新

這是什麼 一個用來將 HTML 文件轉成 PDF 的第三方軟體套件。

為什麼要注意 依全球漏洞預測資料 EPSS，這個漏洞被利用的機率高於 93% 的已知漏洞。攻擊者可能藉由特定的字型設定讓系統去載入不該載入的遠端內容，進而造成資料外洩或讓系統執行不預期的檔案存取。

怎麼處理 請工程或外包團隊先升級到 2.0.1 以上，可解決最要緊的漏洞，但這是跨大版本升級，可能要改程式，建議先排測試。要修掉全部 13 個漏洞，需要升級到 3.1.6 以上。

漏洞編號 CVE-2022-41343、CVE-2023-23924、CVE-2023-50262、CVE-2021-3838、CVE-2022-2400、CVE-2022-0085 等共 13 個

---

laravel/framework `v8.83.16` 排入近期更新

這是什麼 Laravel 是一個用來開發與管理網站應用程式的網頁框架。

為什麼要注意 依全球漏洞預測資料 EPSS，這個漏洞被利用的機率高於 99% 的已知漏洞。攻擊者可能透過特製的網址參數影響框架處理請求時使用的環境設定，進而造成系統以錯誤的方式執行，影響網站功能或資料處理結果。

怎麼處理 請工程或外包團隊先升級到 8.83.28 以上，可解決最要緊的漏洞。要修掉全部 6 個漏洞，需要升級到 12.69.0 以上，這是跨 4 個大版本升級，可能要改程式，建議先排測試。

漏洞編號 CVE-2024-52301、CVE-2026-114509、CVE-2025-27515、CVE-2026-102279、CVE-2026-48019、GHSA-crmm-hgp2-wgrp

© 2026 DataAgent AI Lab

moment `2.29.1` 排入近期更新

這是什麼	JavaScript 的日期處理函式庫，用來解析、驗證、調整與格式化日期。
為什麼要注意	依全球漏洞預測資料 EPSS，這個漏洞被利用的機率高於 97% 的已知漏洞。在特定情況下，攻擊者可能藉由不當輸入影響系統存取路徑，進而讓公司系統讀取到不該讀的檔案內容或造成資料外洩。
怎麼處理	請工程或外包團隊升級到 2.29.4 以上。 `npm install moment@2.29.4`
漏洞編號	CVE-2022-24785、CVE-2022-31129

symfony/http-kernel `v5.4.9` 排入近期更新

這是什麼	一個用來處理網頁請求與回應、並支援共用元件的 PHP Web 框架。
為什麼要注意	依全球漏洞預測資料 EPSS，這個漏洞被利用的機率高於 91% 的已知漏洞。攻擊者可能讀取原本只應該給特定使用者的 Cookie，進而取得使用者的登入狀態，導致公司系統中的帳號或資料被未授權存取。
怎麼處理	請工程或外包團隊升級到 5.4.20 以上。 `composer require -W 'symfony/http-kernel:^5.4.20'`
漏洞編號	CVE-2022-24894

其他要處理的項目

套件	漏洞數	怎麼處理
minimist `1.2.5` 排入近期更新 僅建置用	1	請工程或外包團隊升級到 1.2.6 以上。

需要確認的語言版本

程式庫只寫了宣告的版本，看不到伺服器實際跑的版本，所以這裡不判定有沒有風險。請管伺服器的人確認；網站放在虛擬主機或代管服務的話，請直接問主機商。

語言與宣告版本	請確認什麼
PHP `8.0`	這個系列已停止維護，不會再有修補。請確認伺服器上的 PHP 已升級到 8.3.36 以上。
PHP `8.1`	這個系列已停止維護，不會再有修補。請確認伺服器上的 PHP 已升級到 8.3.36 以上。
PHP `^7.4 || ^8.0`	請依伺服器用的系列確認，至少升級到：8.2 系列 8.2.35（2026-12-31 停止維護）、8.3 系列 8.3.36、8.4 系列 8.4.27、8.5 系列 8.5.12。

© 2026 DataAgent AI Lab

跟著例行更新處理即可

另外有 58 個套件、共 148 個漏洞，預測被利用的機率較低，其中 22 個套件只在開發或建置時用到。這些跟著例行更新處理即可，不需要單獨處理，也不用逐項追問。

下一步

1. 把「重點項目」和「其他要處理的項目」轉給工程或外包團隊，請對方回覆預計完成日期。
2. 請管伺服器的人回覆實際版本，對照「需要確認」的表格。
3. 其餘項目在下一次例行更新時一起升級。
4. 這份報告是掃描當下的結果。新的漏洞每天都在公布，建議定期重新檢查。

想要有新風險時主動通知你？ SupplyGuard 專業版每天重新比對，出現新的高風險時用 LINE、Email 或 Jira 通知，還能產生修補草稿讓工程師審核。 查看方案與價格。

想檢查自己的系統？免費健檢一個程式庫：supplyguard.idataagent.com

這份報告的檢查範圍

看了什麼：程式庫裡的套件鎖定檔，和 Dockerfile 這類宣告語言版本的設定檔，再比對公開的漏洞資料庫、美國 CISA 已知遭利用清單和惡意套件清單。
沒有看什麼：系統自行開發的程式邏輯、伺服器實際安裝的版本、網站對外的設定，也沒有做滲透測試或網址外部檢查。
怎麼解讀：這份報告只涵蓋開源元件的已知風險，不是全面的資安檢測。沒有列出的項目不代表沒有風險。

© 2026 DataAgent AI Lab