WhiteSource Open Source 檢測工具

您知道您所使用的 Open Source 是否安全嗎？

Gartner 調查報告指出，現行企業有80%的應用程式有採用 Open source。
但是多數企業卻無法掌握使用其內所有 Open Source 的版權，版本以及弱點資訊，這對企業是很嚴重的議題，因其高度依賴 Open Source，甚至 OWASP Top 10 也警告使用具有已知弱點的 Open Source 是有危險的，然而絕大多數開發團隊仍然忽視此問題，而非積極確認其引用的 Open Source 是否安全。
駭客透過 Open Source 漏洞可造成大規模且毀滅性的影響，這使得引用 Open Source 的風險逐日俱增。也就是說，一旦 Open Source 的弱點被公布，就會立即變成一個倒數計時的炸彈。

免費總是最貴的，您知道嗎？

80%
現行企業的應用程式
高達 80% 採用
Open Source

86%
高達 86% OSS 弱點可被
駭客進行嚴重破壞的攻擊，
造成大量個資外洩

500,000
OSS 弱點
高達 50 萬個以上

2,300
Open Source 授權多達
2300 種，多數企業不清楚
是否違反 GPL/AGPL 使用方式

Open Source 安全性的挑戰

系統安全測試的技術，像是靜態原始碼檢測，其實無法偵測 Open Source 弱點。因此您需要一套能夠確保 Open Source 元件安全性的解決方案，並可透過 Open Source 社群取得公開資訊，進一步來找出並解決您的弱點問題。好消息是，Open Source 社群透過眾人的努力得以讓 Open Source 的專案在安全上有所保障。

然而基於 Open Source 去中心化的特性，弱點的資訊散落在眾多平台上（NVD, CVE）。這些資訊有些還很難以取得，使得企業單位很難透過人工的方式逐一確認其使用的 Open Source，以及他們的應用程式正遭受弱點攻擊的可能性。

圖說：前十大弱點 Open Source 專案（依弱點數量統計）

此外 Open Source 的相依性也是其挑戰之一。因為透過人力通常無法掌握元件的相依關聯性，且容易在過程中發生人為失誤，企業單位在缺乏完整資訊狀態下，導致難以準確掌握其所使用的 Open Source，也讓自身陷入危險。因此我們建議透過自動化的方式掌握全面資訊，持續監控 Open Source，即時提供對您最切身的訊息，在第一時間採取積極作為，以確保資訊安全。

工具找到漏洞不稀奇，怎麼處理才是問題

WhiteSource 調查報告指出，開發人員一個月花費 15 個小時的時間來解決開源漏洞，相比之下，每月只有花 3.8 小時來修改程式。當開發人員被詢問在發現漏洞時他們做了什麼，他們只提供了大量漏洞資訊，但卻缺乏弱點解決的作業流程。

在處理新發現的漏洞時缺乏標準的處理作法，這說明了在解決開源漏洞時是非常沒有效率的。解決開源漏洞的策略，應該是確保公司按時解決最關鍵或是最重要的漏洞問題。

專家一致認為，要試著每個弱點問題都解決其實是很困難的，關鍵是把問題的優先順序找出來，進而解決最急迫性的。

關於 WhiteSource

該公司成立於 2008 年，是唯一將 Open Source 元件的授權、安全性、品質及管理等所有功能集結在一起的 Open Source 管理工具。作為值得信賴的軟體開發組件分析 (Software Composition Analysis, SCA) 的領導廠商，WhiteSource 幫助產業的龍頭像是微軟、IBM、Comcast 和其他數百家企業，利用他們的開源技術持續在 Open Source 領域對於安全及合規提供有效的解決方案。

產品介紹

WhiteSource 是一套 Open Source 管理工具，透過它即可知道，Open Source 的安全、品質及授權。它可線上即時操作，通過自動、持續的掃描方式，與後端數十個 Open Source 資料庫進行比對；與資料庫交叉比對的結果，辨識您的第三方元件是否有弱點，版本更新狀況及 License 有效性。

支援的語言及工具

FORRESTER

The Forrester WaveTM 於 2019 年”Software Composition Analysis (SCA)”報告中，WhiteSource 榮獲 Open Source 管理工具第一名。

自動化才是王道

WhiteSource 加入 SDLC 流程：提供您自動化管理機制，掌握安全、品質、License compliance policies，以應付弱點和有問題的元件。

Shift Left & Shift Right：Shift Left 協助團隊減少成本，以及因提早發現問題而可爭取修復時間。WhiteSource 可以在您瀏覽Open Source 的同時 (Web Advisor)，提供完整資訊供開發人員評估，在開發前期及掌握最新且完整的資訊。Shift Right－WhiteSource 可持續、自動化監控您所部署的系統，提供最即時的完整資訊。

整合 Open Source 安全到 CI/CD 流程：WhiteSource 可整合至軟體開發和測試平台，以優化您軟體開發流程，Open Source 自動化的全面管理，包含 Open Source 的挑選、確認、偵測和修復弱點。

WhiteSource 產品獨特之處

弱點偵測

準確的偵測功能是必要的——您在一無所知的狀況下，無法解決實際的核心問題。
我們能為您找出您使用的 Open Source 帶來的所有弱點。

找出對您有影響的弱點：

WhiteSource Prioritize (前身為 Effective Usage Analysis, EUA) 可指出回報的弱點是否確實被程式碼所引用，可降低七成誤判的發生，並將弱點等級依照風險程度分級；假如顯示確實有影響，將提供弱點發生確切位置，利於開發人員在短時間內有效處理關鍵問題。經過 WhiteSource 的研究指出，公司自行開發程式所引用的 Open Source 弱點掃描結果近七成為誤判。導致您總是花費時間與團隊精力處理不重要的弱點，無法在短時間內針對關鍵問題及時處理。

終結誤判：

拜演算法所賜，WhiteSource 可比對已知的弱點與確實有被影響到的 Open Source，確保沒有誤判的情形發生。因此可將開發團隊的時間和資源更有效的利用。

支援度：

200+ 語言：WhiteSource 的資料庫 (包含 CVE/NVD、多元的 Security advisories、以及常見的 Open Source 問題追蹤網站) 涵蓋最廣泛的弱點資訊，支援超過 200 種程式語言，搭配持續監控的自動化機制，可有效掌握最即時且完整的狀況，提供能見度給使用者決策。

弱點修復

挑戰一　駭客在使用漏洞攻擊 Open Source 弱點的速度越來越快，又以常見的 Open Source 為攻擊標的。

挑戰二　對於開發人員而言，要能掌握完整資訊，快速完成修復問題，不影響現有功能運作，更是難上加難。

指出弱點發生的位置：

提供完整程式流程路徑分析，指出程式中弱點實際的位置。掌握關鍵性的洞悉能力，可以讓開發人員在尋找與修復弱點時更有效率。

建議修復：

除了 Open Source 社群上公布的弱點之外，WhiteSource 研究團隊更進一步去分析所有弱點資料庫，找出有潛在資安風險弱點的 Open Source，為您提供更完整的資訊；提供版本比較功能，讓修復弱點時找出對企業影響最小且無安全疑慮之版本。

自動化流程：

針對每一次更新後找到的弱點，透過自動觸發問題管理的機制，確保在每一次通報的緊急狀態下，修復流程的每一個環節都能有效被追蹤。

WhiteSource Prioritize

“資安團隊遵守其職，然而無效弱點的舉報，成為開發團隊的絆腳石，牽制開發進度且花費精力在處理誤判、低風險或是未直接影響系統的問題。”

(10 Things to Get Right for Successful DevSecOps Neil MacDonald, Gartner)

把問題找出來很容易，但是你更需要知道的是「哪些弱點對你是確實有影響」。

這就是 WhiteSource 研發出 Prioritize 的目的，透過有效分析，將弱點按照風險高低分級，提供給您的開發團隊最關鍵的資訊，使其能在短時間內有效地正視與解決問題。

Prioritize 提供完整的弱點呼叫流程分析，簡化您修復弱點的流程。透過 Prioritize 分析，資安與開發團隊可以更專注在解決”確切”的問題，且能進一步掌握準確且詳細的弱點修復資訊，提高管理 Open source 的效率。

WhiteSource Prioritize

確實指出回報的弱點已被程式碼所引用，因此能快速提升弱點的能見度。專注在“確實對您有影響”的弱點，比起過去工具總是幫您找出一堆未經分析的弱點，Prioritize 可以節省您寶貴的時間和精力，在開發的同時兼顧您的系統安全強度，創造資安與開發團隊的雙贏。

WhiteSource Prioritize 技術說明

經由靜態程式分析演算法（ 專利申請中 ），只需一杯咖啡的時間，即可產出精準的分析報告，並大幅降低誤判的發生。支援高階語言使用模型（polymorphism, pointer calls, virtual tables, and more.）。Prioritize 依照風險程度高低將弱點分類，讓您一目了然現況分析。它可直接透過 WhiteSource Unified Agent 進行掃描，分析的結果直接在 WhiteSource 網站來呈現，也產出報告。經研究指出，透過有效分析來管理 Open source，可減少近七成的誤判，掌握有效資訊，您即可以更從容地、專注在處理確實的問題。

WhiteSource Prioritize 產品特色

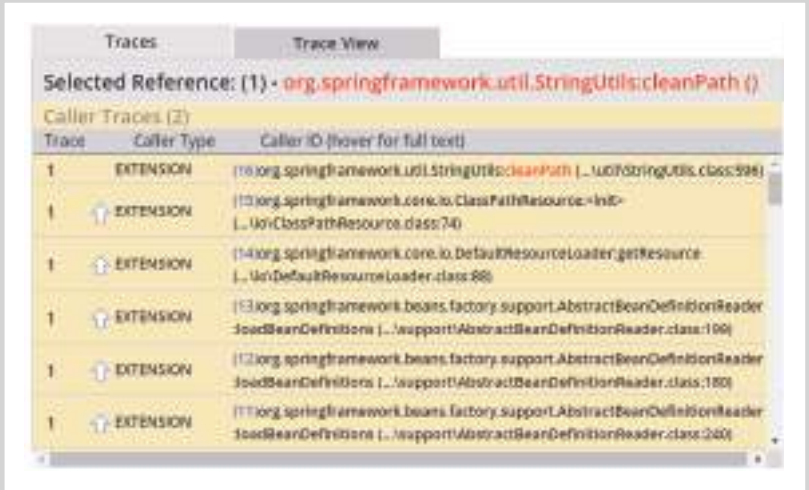
●取得資訊：擁有豐富的資源，以找到企業私有 Open Source 程式的弱點。

●風險分類：對回報弱點風險分級警示，Open Source 被發現存在 1 個具有高嚴重性的弱點；透過 Prioritize 則發現程式碼並未實際有引用該 Open Source，因此對系統不會產生任何影響。可從標誌顏色以及括號內所顯示的弱點數（透過 Prioritize 分析）判斷弱點的影響程度。

●弱點辨認：提供弱點確切位置，弱點所在資料夾檔名、行數、呼叫路徑（call traces），具備這些資訊，開發人員可以透過多種方法來解決問題，例如註解程式碼，或跳過呼叫此弱點的程式碼。

●視覺化呈現：從企業專屬的 Open Source 程式碼，追蹤到呼叫發生問題的 Open Source，並呈現清楚的程式路徑。

●影響評估：了解”確實會產生影響的弱點”在所有弱點所佔比例，對開發人員而言在修弱點的工作上可提升效率，將時間與精力專注在”實實的弱點”。



WhiteSource Prioritize 分析指標

此弱點和程式存在
直接或間接的關係
（需修復）

資訊不足，
無法確認弱點是否有效
（可能因資料不足）

此通報的漏洞，
程式未引用，不受影響。
（不需修復）

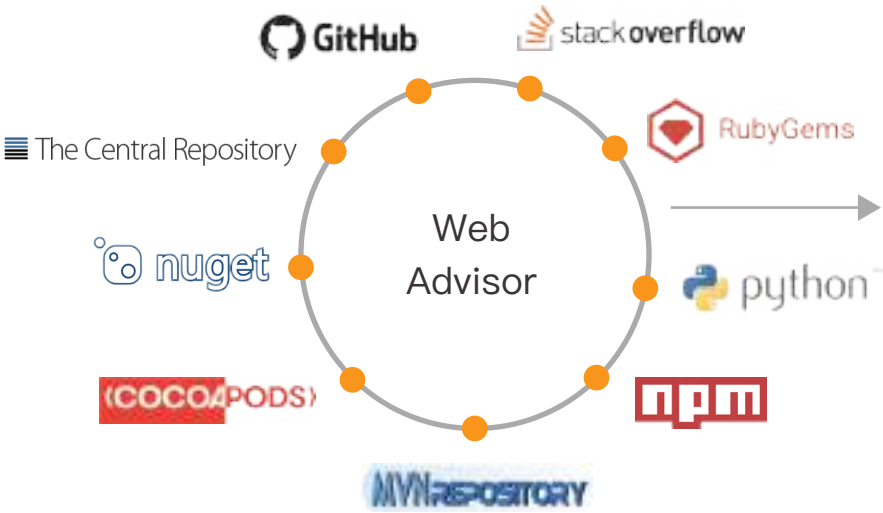
因弱點資訊更新，
建議您再重新執行掃描

WhiteSource Web 介面

儀表板資訊－透視元件，一覽無遺，快速找到有問題的 Open Source

Open Source 詳細資訊－找到最安全且最適合更新的版本

Web Advisor －落實 Shift Left 針對各大開源資料庫網頁立即進行掃描，確認無弱點、授權或違反公司政策問題。



台灣某企業（電信業）

李進河 技術服務處 經理：「導入 WhiteSource，不僅能將系統的整合與測試行為融入開發系統的過程中持續進行，透過自動化建置、程式碼分析與測試，輔助專案進度掌握，更能提升專案的品質，讓我們能提供客戶更完整的檢測服務。」

TEMENOS（銀行業）

馬丁•貝利 產品總監 企業軟體部：「使用 WhiteSource 我們將所有的 Open Source 元件進行全面清查，並能確保完全符合我們的許可政策。現在，我們可以迅速地回答前端的任何問題，肯定我們是 100% 準確的，都沒有浪費任何我們的開發的寶貴時間。」

PANORAMIC POWER（製造業）

在嵌入式軟體中管理 Open Source 元件 Gev Decktor VP 軟體開發部：「敏捷式架構和高要求的生態系統，讓我們必需使用類似 WhiteSource 自動化管理我們的 Open Source 元件、依賴性和版本的解決方案。」

HYPE（SDLC 創新管理軟件的全球領導者）

AAlbrecht Scheildig 產品開發部負責人：「使用 WhiteSource 我們可以為客戶提供最新的 Open Source 報告，而這一切需要按一下按鈕。

GSS IT & Security

APPERIAN MOBILE APP MANAGEMENT

ARXAN

CHECKMARX choose what developers use

kryptowire

WhiteSource

GSS 叡揚資訊 Galaxy Software Services

國家產業創新獎
卓越中堅企業獎

成立於 1987 年，是台灣資訊軟體業的領導廠商，於應用系統開發已有 20 餘年經驗，擁有超過 300 位軟體開發人員資源。

2006 年率先投入源碼檢測領域，2012 年引進新一代源碼檢測工具 Checkmarx，迄今累積了逾 100 家客戶豐富經驗（包括政府、金融保險證券、國營企業、大專院校、資訊服務業等私人企業）。

服務範圍：包括源碼檢測服務、工具使用建置及建議、SSDLC 整合、軟體 Coding 安全課程等，協助客戶提升應用系統安全強度。

台 北 總 公 司　10461 台北市中山區德惠街 9 號 5 樓
Tel: +886-2-2586-7890　Fax: +886-2-2586-8787

高 雄 辦 公 室　80453 高雄市鼓山區明華路 317 號 6 樓
Tel: +886-7-5866195

www.gss.com.tw