確保軟體開發的基礎

隨著國家支持的網路攻擊和網路惡意行為者急劇增加，我們相信我們的產品和服務只有在安全的情況下才能發揮作用。在 Google，我們比以往任何時候都更加著重在保護民眾、組織和政府，透過分享我們的專業知識，賦能社會，讓社會應對不斷變化的網路風險，且致力於推動網路安全的技術，為每個人打造更安全的世界。

開源軟體：任何人都可以免費使用、修改和建構的程式碼，是現代網際網路的基礎。開源軟體開發的世界可以自由分享解決方案，以進行協作並快速創新。然而，正是這種開放性讓每個人都可以存取數位世界，但也使開源軟體特別容易受到安全威脅。

挑戰

開源軟體是每個人都關心的議題

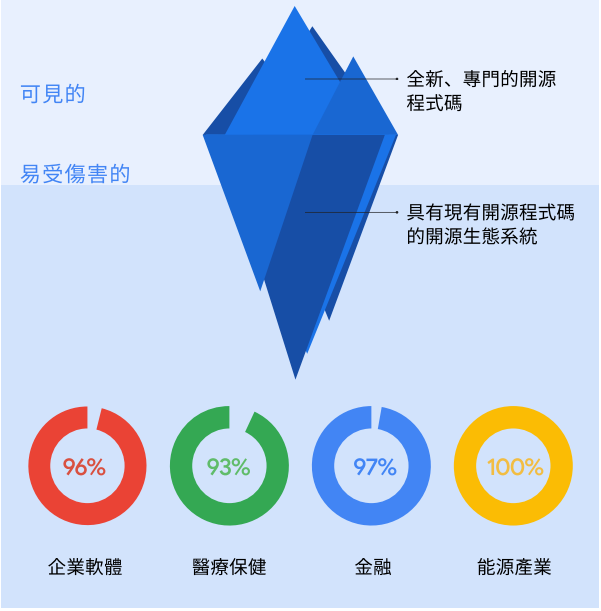
建立在透明和分享基礎上的開源開發社群，為我們今日使用的大多數應用程式貢獻了大量的程式碼。從醫療設備到電網，人們幾乎每天無時無刻都依賴開源軟體 (OSS)，使得開源專案成為網路攻擊的主要目標。在過去三年中，軟體供應鏈攻擊較前一年同期相比成長了 742%[1]。

開源生態系統錯綜複雜，其中隱藏的間接依賴關係可能帶來安全漏洞。這些層級使得漏洞難以手動檢測，而保護這部分的軟體開發已成為全球緊迫的安全問題。

各層級都需要額外關注：

- 開源開發人員需要知識和資源來保護他們的專案
- 組織需要了解供應鏈風險和漏洞，以制定減緩計畫
- 政府和產業必須攜手落實穩健、有效的安全標準[3]

包含開源程式碼的工業軟體百分比[2]



[2] 來源: 2022 Synopsys Open Source Security and Risk Analysis Report

我們的解決方案

為每個人保護開源軟體

Google 多年來一直致力於克服這一挑戰。事實上，每年都有超過 10% 的 Google 員工提供開源軟體專案。從我們的經驗得知，實際上可以透過採納開放來實現現代數位安全。開放的方法能確保我們能夠快速採用最新的創新技術，並協助更多人解決安全挑戰。但要充分發揮開源軟體的價值，我們需要更強大的公私合作夥伴關係和動態政策框架，來為每個人的安全提供支援。這就是為什麼我們樂見美國政府為推進 OSS 安全所做的努力，例如參議院於 2022 年提出了《保護開源軟體法案》。

- 我們正藉由更高級別的安全框架引領社群，例如軟體工件的供應鏈級別 (SLSA)，[4,5] 並開發進階安全工具。
- 我們開發了 Graph for Understanding Artifact Composition (GUAC)，將來自不同來源的軟體安全資訊匯集到單一個可查詢的資料庫中。GUAC 將安全資訊的可用性大眾化，讓每個組織都可以免費存取並使用安全資訊。

我們的承諾：

- 投資 1 億美元於開源安全性，在開源安全基金會中擔任領導職務，並與開發人員直接合作
- 定義並提供可操作的安全標準、指南、我們在內部使用的免費工具和最佳實踐，與整個開源社群分享
- 預先檢測、自動分類以及於最早開發階段建構安全性的方法
- 自動化工具，讓每個人都能免費獲得企業級安全

應用程式

Google OSS Fuzz
我們對心臟出血漏洞 (Heartbleed) 錯誤的回應

Heartbleed 錯誤是一個嚴重的開源漏洞，它是可能會影響幾乎所有網際網路使用者的缺點。2014 年，駭客從美國最大型醫院中其中一家的資料庫中竊取了大約 450 萬名患者的姓名、地址、出生日期、電話號碼和社會安全號碼

為了處理此問題，Google 推出了 OSS-Fuzz，提供為免費社群服務。與可能需要數月的手動測試不同，模糊測試可在幾分鐘內查明未知的安全漏洞。我們投資建立了一個基礎設施，自動測試數百個開源專案。OSS-Fuzz 現在會定期執行程式碼掃描，並持續創新，以發現更多類別的錯誤。

以六種語言的模糊測試掃描了 800 多個關鍵開源專案。

我們的產業投資和里程碑

2020 八月
加入開源安全基金會 (OpenSSF)，引導並提高開源軟體的安全性

2021 五月與六月
根據白宮行政命令 14028 建立了 OSS 最佳實踐，並提供完善軟體供應鏈安全標準的建議。

六月
使用 OpenSSF 發布 SLSA，將 Google 的內部安全框架外部化，讓每個人都可以建構更安全的軟體。

八月
承諾投入 1 億美元提升並保護 OSS，包括與開發人員合作，尋找並修復漏洞

2022 五月
在 DC 峰會期間 **宣布成立 Google 的開源維護團隊**，指派一支專職開發人員團隊直接負責開源專案，以提高其安全性。

五月
宣布推出 Assured Open Source Software 產品，協助將 Google 使用的相同可信開源軟體組整合至開發人員工作流程中。

Google 推薦的做法現今能協助公私組織維持安全性：

- 實施 SLSA，加強軟體供應鏈安全
- 使用 Sigstore 加密簽名並驗證軟體的真實性
- 使用 OSS-Fuzz 和 OSV.dev 自動發現、追蹤並分類漏洞
- 使用記分卡自動評估相依項目的安全風險

我們的方法

軟體的安全取決於最薄弱的環節。我們挹注專業知識和財務資源，提升整個開源生態系統的安全性。我們的開發和安全專家團隊相信，我們可以透過以下方式保護更多的公私組織：

我們的團隊審核產品生命週期的每個階段，持續掃描、分析並模糊測試漏洞

我們支援開放的網際網路，與開發者社群分享我們手上的資訊，並為公眾和企業維護安全

我們透過檢測複雜的威脅、提供先進的自動化工具，並在未來發生的任何狀況中保持領先地位，超前部署安全性

保護開源軟體是共同的責任，我們致力於在這項緊迫、關鍵的問題上持續合作。
g.co/security/gosst

資料來源: 1. 2022 State of the Software Supply Chain。2. 2022 Synopsys Open Source Security and Risk Analysis Report。3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules。4. 分享我們的知識 (即發布 SLSA、指導 OpenSSF) 代表每個開發軟體的人，而不僅僅是 Google，都可以從 Google 的經驗和禁得起時間考驗的安全實踐中受益。5. SLSA 是一組可以協助組織提高其軟體開發過程安全性的實踐。這組實踐符合美國政府的安全軟體開發框架，該框架是政府為響應網路安全行政命令而訂定的要求。這代表各組織將獲得有關如何遵守聯邦準則的協助，創造對所有人都更安全的軟體。