Software Security Research 發佈公告

Fortify 軟體安全性內容

2022 更新 3

2022 年 9 月 30 日

關於 CyberRes Fortify Software Security Research

Fortify Software Security Research 團隊將尖端研究成果轉變為可為 Fortify 產品組合 (包括 Fortify Static Code Analyzer (SCA) 和 Fortify WebInspect) 增添動能的安全情報。現在，Fortify 軟體安全性內容能夠跨 30 種程式設計語言支援 1,244 個弱點類別，且涵蓋 100 多萬個單獨 API。

Fortify Software Security Research (SSR) 欣然宣布，現已推出以下產品的更新：Fortify Secure Coding Rulepacks (英文，2022.3.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)，以及 Fortify Premium Content。

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

隨著此發佈，Fortify Secure Coding Rulepacks 能夠跨 30 種程式設計語言偵測 1,024 種獨特的弱點類別，且涵蓋 100 多萬個單獨 API。概括地說，此發佈包含下列項目：

ASP.NET Core 更新 (支援的版本：6.0)[1]

在 Model-View-Controller (MVC) 模式中，視圖是使用內嵌在 Razor 標記中的 C# 程式設計語言的 *.cshtml* 檔案。Razor 標記是與 HTML 標記互動的程式碼，用於產生傳送給用戶端的網頁。視圖會處理應用程式的資料呈現與使用者互動。使用 Fortify Static Code Analyzer 22.2.0 版及更高版本時，規則現在支援在視圖中尋找問題。

支援包括下列弱點類別的涵蓋範圍：

- ASP.NET MVC Bad Practices: Form Without AntiForgery Token
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Open Redirect
- Privacy Violation
- System Information Leak

Entity Framework Core (支援的版本：6.0)

Entity Framework (EF) Core 是一種開放原始碼資料存取技術，適用於 .NET 應用程式。EF Core 允許開發人員將 .NET 物件對應到資料庫結構描述，並透過標準 API 和 LINQ 查詢叫用資料庫作業。支援包括下列弱點類別的涵蓋範圍：

- Access Control: Database
- ASP.NET Bad Practices: Leftover Debug Code
- Connection String Parameter Pollution
- Insecure Transport: Database
- Password Management: Hardcoded Password
- Setting Manipulation
- SQL injection
- System Information Leak: Overly Broad SQL Logging

[1] 需要 Fortify Static Code Analyzer 22.2.0 版或更高版本。

GitHub Actions

GitHub Actions 是一種持續整合與持續傳遞 (CI/CD) 平台，可實現建置、測試和部署管道的自動化。最近發現的弱點會導致各種系統存在 Command Injection 攻擊媒介。此版本包括在下列類別下偵測此 Command Injection 弱點的常見執行個體涵蓋範圍：

- Command Injection: GitHub Actions

React (支援的版本：18.2)[2]

React 或 ReactJS 是一種開放原始碼 JavaScript 程式庫，用於建置以元件為基礎的使用者介面。雖然此版本不支援新的弱點類別，但已重新修改涵蓋範圍，使 React 更為準確並減少誤報。

React Native (支援的版本：0.70)[2]

React Native 是一種開放原始碼 UI 架構，用於在 JavaScript 和 JSX 中開發多平台使用者介面。React Native 讓開發人員能編寫由目標平台原生轉譯 API 進行轉譯的行動應用程式，以產生平順且一致的使用者體驗。除了 React 支援的弱點類別外，我們也為 React Native 新增了下列弱點類別：

- Open Redirect
- Privacy Violation
- System Information Leak: Internal

React Native Async Storage (支援的版本：1.17)[2]

Async Storage 是一種未加密、非同步、鍵值儲存庫，適用於以社群 *react-native-async-storage project* 為基礎的 React Native。Async Storage 在原生 iOS 和 Android 平台的特定儲存機制的頂層提供抽象化功能。支援透過 Async Storage 實現資料流通，並回報現有 JavaScript 和平台/程式庫特定的弱點類別。

Secret Scanning 改進

Secret Scanning 是一種在各種原始程式碼和組態檔案中尋找 Secret 的概念。Fortify Static Code Analyzer 會將 Secret Scanning 涵蓋範圍套用於所有檔案類型，藉此允許尋找特定的 Secret，而不管程式碼語言為何。已新增對下列 Secret 的支援，並且會回報為 *Password Management: Hardcoded Password* 或 *Credential Management: Hardcoded API Credentials*:

- HTTP Basic 驗證權杖
- JWT (JSON Web Tokens)
- NPM (Node Package Manager) 存取權杖
- Postman API 金鑰
- PyPI API 權杖

---

2 需要 Fortify Static Code Analyzer 22.2.0 版或更高版本。

對 Java 和 Go 的初始 gRPC 支援 (支援的版本：1.49.0)

Google Remote Procedure Call (gRPC) 是一種現代多環境、多語言的開放原始碼高效能 RPC 架構。gRPC 可連接支援負載平衡、追蹤和驗證的服務。有別於傳統的 JSON-over-HTTP，gRPC 以 HTTP2 為基礎，並且通常使用二進位通訊協定緩衝 (protobuf) 格式的訊息。對於 gRPC 專案，使用者應在 Fortify Static Code Analyzer 的轉譯階段期間，將 .proto 檔案定義產生的程式碼包括在內。

已新增對 Go gRPC v1.49.0 的支援以涵蓋下列弱點類別：

- Header Manipulation
- Privacy Violation
- System Information Leak: External

已新增對 Java gRPC v1.49.0 的支援以涵蓋下列弱點類別：

- Denial of Service
- gRPC Metadata Manipulation
- Insecure Transport
- Insecure Transport: gRPC Server Credentials
- Insecure Transport: gRPC Channel Credentials
- Privacy Violation
- Resource Injection
- System Information Leak: External

初始 Flask 支援 (支援的版本：2.2.x)

Flask 是一種以 Python 編寫而成的 Web 架構。Flask 最初是適用於 *Werkzeug* 和 *Jinja* 程式庫的包裝函式，現已成為最熱門的 Python Web 應用程式架構之一。為了輔助我們對 Python 的 Google Cloud Functions 支援，此版本僅包含對 Flask Response 物件的支援。
支援包括下列弱點類別的涵蓋範圍：

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Permissive SameSite Attribute
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Unenforced Content Security Policy
- Open Redirect

- Privacy Violation
- System Information Leak: External

Google Cloud Functions (支援的版本：403.0.0)

Google Cloud Functions 是一個可以建置並連接雲端服務的無伺服器執行環境。它可以執行程式碼以回應預先定義的事件，例如 API 呼叫、資料庫交易、將檔案上傳到 Cloud Storage，或 Cloud Pub/Sub 主題的傳入訊息。
Cloud Functions 提供兩個產品版本：Cloud Functions (第 1 代) 即原始版本，以及 Cloud Functions (第 2 代)，這個新版本以 *Cloud Run* 和 *Eventarc* 為基礎建置而成，可提供增強的功能集。此版本包括對 Python 中 Google Cloud Functions 的支援以及更新對 Java 中 Google Cloud Functions 的支援。

Python 支援的弱點類別包括 Flask API 支援的弱點類別，以及下列類別：

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Privacy Violation
- System Information Leak: External

對於 Python Google Cloud Functions，使用者應包含 JSON 或 YAML 雲端建置檔案。或者，使用者也可以在掃描時設定下列屬性：

- *com.fortify.sca.rules.GCPFunctionName* 應設為函式名稱。
- 如果觸發類型為 HTTP，則 *com.fortify.sca.rules.GCPHttpTrigger* 應設為 `true`，若為其他觸發類型，則應設為 `false`。

在更新對第 2 代 Java Google Cloud Functions 的規則支援後，現在可辨識源自 CloudEvents 要求的危險輸入來源。

初始 Apollo Server 支援 (支援的版本：3.6.8)

Apollo Server 是一種開放原始碼 GraphQL 伺服器，用於 JavaScript 應用程式以建置 GraphQL API。此版本增加了對 Apollo Server 的初始 GraphQL 伺服器支援，包括在使用 Apollo Server 開發的 GraphQL API 中偵測下列弱點類別：

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- Privacy Violation
- System Information Leak: External

基礎架構即程式碼 (IaC)

IaC 是透過程式碼管理和佈建電腦資源的程序，而非各種手動程序。支援的技術包括用於部署到 GCP、OpenAPI 規範和 MuleSoft 的 Terraform 組態。目前已將與上述服務組態設定相關的常見問題回報給開發人員。

Google Cloud Platform (GCP) Terraform 組態

Terraform 是一種開放原始碼 IaC 工具，用於建置、變更及版本化雲端基礎架構。它使用自己的宣告式語言，稱為 HashiCorp Configuration Language (HCL)。雲端基礎架構會被編碼到組態檔案中，用以描述所需的狀態。Terraform 提供者可支援 GCP 基礎架構的設定及管理。此版本涵蓋 GCP Terraform 組態的下列弱點類別：

- GCP Terraform Misconfiguration: Cloud SQL Database Publicly Accessible
- GCP Terraform Misconfiguration: Cloud Storage Bucket Uniform Access Disabled
- GCP Terraform Misconfiguration: Compute Engine IP Forwarding Enabled
- GCP Terraform Misconfiguration: Compute Engine Serial Console Enabled
- GCP Terraform Misconfiguration: Compute Engine Shielded VM Option Disabled
- GCP Terraform Misconfiguration: GKE Cluster Node Auto-Repair Disabled
- GCP Terraform Misconfiguration: GKE Cluster Publicly Accessible
- GCP Terraform Misconfiguration: Overly Permissive Role
- GCP Terraform Misconfiguration: Permissive Firewall

OpenAPI 規格

OpenAPI 規格針對 HTTP API 定義了一個標準、與程式設計語言無關的說明。符合 OpenAPI 規格的 OpenAPI 文件可以用 JSON 或 YAML 格式來表示。此標準定義了在無需存取實作、說明文件或透過網路檢查的情況下，服務提供哪些功能。此版本涵蓋 OpenAPI 組態的下列弱點類別：

- OpenAPI Misconfiguration: Credential Leakage
- OpenAPI Misconfiguration: Empty Global Security Requirement
- OpenAPI Misconfiguration: Empty Operation Security Requirement
- OpenAPI Misconfiguration: Insecure Transport
- OpenAPI Misconfiguration: Missing Error Handling
- OpenAPI Misconfiguration: Missing Global Security Requirement
- OpenAPI Misconfiguration: Missing Operation Security Requirement
- OpenAPI Misconfiguration: Missing Security Schemes
- OpenAPI Misconfiguration: Optional Global Security Requirement
- OpenAPI Misconfiguration: Optional Operation Security Requirement
- OpenAPI Misconfiguration: Weak Authentication

Mule

Mule Runtime 通常簡稱為 Mule，是 MuleSoft 提供的企業服務匯流排與整合架構。Mule 支援整合現有的系統，例如 Web 服務、HTTP、Java Database Connectivity (JDBC) 等。Mule 可以當成企業網路內或網際網路上應用程式之間的傳輸系統，藉此允許不同的應用程式相互通訊。此版本涵蓋 Mule 組態的下列弱點類別：

- Mule Misconfiguration: Hardcoded Password
- Mule Misconfiguration: Insecure Database Transport
- Mule Misconfiguration: Insecure Transport
- Mule Misconfiguration: Server Identity Verification Disabled

2022 CWE Top 25

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) 於 2019 年推出，取代了 SANS Top 25。6 月發佈的 2022 CWE Top 25 是使用啟發式公式決定的，這個公式會將過去兩年回報給美國國家弱點資料庫 (National Vulnerability Database，NVD) 的弱點頻率及嚴重性正規化。為了支援我們的客戶，使其可以針對 NVD 中最常回報的重大弱點排列稽核作業的優先順序，已新增 CyberRes Fortify Taxonomy 與 2022 CWE Top 25 之間的關聯性。

其他勘誤

在此發佈中，我們已投入一切資源，來確保我們可以降低誤報問題數、針對一致性完成修改，並提升客戶稽核問題的能力。客戶還會看到與下列各項相關回報問題的變更：

不再支援 19.x 之前的 Fortify Static Code Analyzer 版本

正如 2021.4 版所觀察到的，我們將繼續支援 Fortify Static Code Analyzer 的最後四個主要版本。因此，這將是支援 19.x 之前的 Fortify Static Code Analyzer 版本的最後 Rulepack 版本。在下一個版本中，Fortify Static Code Analyzer 19.x 之前的版本將不會載入最新的 Rulepack。此時將會要求降級 Rulepack 或升級 Fortify Static Code Analyzer 版本。在未來的版本中，我們將繼續支援 Fortify Static Code Analyzer 的最後四個主要版本。

基礎架構即程式碼 (IaC) 弱點類別

隨著支援偵測與 IaC 相關的錯誤組態和不良做法逐漸成熟，我們的下一個安全性內容版本將包括對弱點類別子集進行類別名稱變更 (2022 更新 4)。當弱點類別名稱發生變更時，若將先前掃描與新掃描合併，掃描結果將會導致類別的增加/移除。

針對弱點類別修改 Fortify 優先順序中繼資料

隨著應用程式安全領域日益成熟，我們對弱點類別對機密性、完整性和可用性的影響的集體知識和理解也在不斷發展。我們下一個版本的安全性內容將包括對弱點類別子集的弱點中繼資料欄位「accuracy」和「impact」進行變更 (2022 更新 4) 。當弱點中繼資料欄位發生變更時，之後的掃描結果可能會在不同的篩選集資料夾 (例如嚴重、高、中、低) 中出現問題。初始更新會造成一些問題從較高的 Fortify Priority Order (FPO) 資料夾轉移到較低的 FPO 資料夾。客戶應該針對這種變更會如何影響現有篩選集和範本做好準備。

誤報改進功能

我們在此版本中持續著手移除誤報。除了其他改進之外，客戶還可以期待在以下領域看到誤報已進一步移除：

- *Cross-Site Request Forgery* – 已移除在 .NET 應用程式中使用 4.5.2 版以上的 .NET Framework 時會出現的誤報
- *JavaScript Hijacking* – 問題 (請參閱下節)

- *Key Management* – 已減少 JavaScript 掃描中的誤報
- *Key Management* – 已減少主要會影響 SAPUI5 專案的誤報
- *Key Management* – 已移除比較問題所產生的大量誤報
- *Password Management: Hardcoded/Empty/Null Password* – 已防止 C# 條件式陳述式的誤報
- *Password Management* – 已減少來自 NPM、Yarn 和 Bower 檔案的誤報
- *Privacy Violation: Autocomplete* – 已減少設定新密碼時的誤報
- *Setting Manipulation* – 已減少清除環境變數時的誤報
- *Weak Cryptographic Signature* – 已防止 java.security 套件中的誤報
- *XML Entity Expansion Injection* – 已減少使用 JAXP 轉換器時 Java 程式中的誤報

JavaScript Hijacking 移除

下列類別在最新 ECMAScript 中不再相關並已移除：

- JavaScript Hijacking
- JavaScript Hijacking: Constructor Poisoning
- JavaScript Hijacking: Vulnerable Framework

因此，上述類別的所有問題都會從掃描結果中移除。

類別變更

除了移除誤報之外，我們也找到一些類別應予以統一或有標籤錯誤的問題。當弱點類別名稱發生變更時，若將先前掃描與新掃描合併，掃描結果將會導致類別的增加/移除。

- *Insecure SSL: Android Hostname Verification Disabled* 現在會回報為 *Insecure SSL: Server Identity Verification Disabled*
- 在 Dockerfiles 中，*Password Management: Hardcoded Password* 問題現在會回報為 *Password Management: Password in Configuration Files*
- 在 .NET 中，設定資料庫連線字串時，部分 *Setting Manipulation* 執行個體現在會回報為 *Connection String Parameter Pollution*

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 將數千個弱點的檢查，與在透過 SmartUpdate 立即取得的以下更新中引導使用者的原則結合在一起：

弱點支援

Insecure Deployment: Unpatched Application

dotCMS 是一種內容管理系統，其提供在一個集中位置建立及重複使用內容、影像和資產的能力。ContentResource API 易受 CVE-2022-26352 所識別出的遠端程式碼執行 (RCE) 漏洞攻擊。用於儲存內容的檔案名稱是使用多組件要求中提供的使用者輸入來建構，並且不會被 dotCMS 清理。

這會使攻擊者能夠在系統上上傳任意檔案，進而導致 RCE。此版本包含一項檢查功能，可用於偵測執行受影響 dotCMS 版本的目標伺服器上是否有此漏洞。

Insecure Deployment: Unpatched Application

Apache APISIX 是一種開放原始碼 API 閘道，提供負載平衡、動態上游等流量管理功能。此 API 閘道易受 CVE-2022-24112 所識別出的 RCE 漏洞攻擊。攻擊者可以透過批次要求外掛程式，來略過 Apache APISIX 的 IP 限制。如果 APISIX 使用預設的 Admin 金鑰，並且啟用了 Admin API 而沒有指派自訂管理連接埠，則攻擊者可以透過批次要求外掛程式來叫用 Admin API，進而導致 RCE。此版本包含一項檢查功能，可用於偵測執行受影響 Apache APISIX 版本的目標伺服器上是否有此漏洞。

Dynamic Code Evaluation: JNDI Reference Injection[3]

Java Naming and Directory Interface (JNDI) 是一種 Java API，能使用戶端依名稱探索及查詢資料和物件。這些物件可以透過不同的命名或目錄服務進行儲存和擷取，例如遠端方法叫用 (RMI)、通用物件請求代理架構 (CORBA)、輕量型目錄存取通訊協定 (LDAP) 或網域名稱服務 (DNS)。如果攻擊者取得控制權，可以控制傳送至 JNDI 查詢作業的引數時，便可以將查詢指向他們控制下的命名或目錄服務，並傳回使用遠端處理站以進行物件具現化的 JNDI 參考。這種攻擊可以在執行查詢作業的目標伺服器上執行任意遠端程式碼。此版本包含一項檢查功能，可用於偵測目標伺服器上是否存在此漏洞。

Dynamic Code Evaluation: Unsafe Deserialization[3]

CVE-2022-21445 已識別出在 Oracle Fusion Middleware 12.2.1.3.0 和 12.2.1.4.0 版的 ADF Faces 元件中，存在一個預先授權的不安全 Java 還原序列化漏洞。它會影響所有依賴 ADF Faces 元件的應用程式，包括 Business Intelligence、Enterprise Manager、Identity Management、SOA Suite、WebCenter Portal、Application Testing Suite 和 Transportation Management。此問題會讓攻擊者能在伺服器上執行任意程式碼、濫用應用程式邏輯或發動 Denial of Service (DoS) 攻擊。此版本包含一項檢查功能，可用於偵測目標伺服器上是否存在此漏洞。

合規報告

2022 CWE Top 25

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) 於 2019 年推出，取代了 SANS Top 25。6 月發佈的 2022 CWE Top 25 是使用啟發式公式決定的，這個公式會將過去兩年回報給美國國家弱點資料庫 (National Vulnerability Database，NVD) 的弱點頻率及嚴重性正規化。

[3] 需要 WebInspect 21.2.0.117 或更高版本修補程式中提供的 OAST 功能。

此 SecureBase 更新納入了直接對應到 CWE Top 25 所識別的類別的檢查，或是透過「ChildOf」關係對應到 Top 25 中 CWE-ID 相關的 CWE-ID。

原則更新

2022 CWE Top 25

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 2022 CWE Top 25 相關的檢查而自訂的原則。

其他勘誤

在此版本中，我們已投入一切資源，以進一步降低誤報數，並提升客戶稽核問題的能力。客戶還會看到與下列各項相關回報結果的變更：

Dynamic Code Evaluation: Unsafe Deserialization[4]

由 ID 11504 所識別的檢查已修改為使用支援 OAST 功能的有效酬載。改進此檢查可減少誤報並提高其結果的效率和準確性。

Fortify Premium Content

研究團隊在我們的核心安全情報產品之外建置、延伸並維護各種資源。

2022 CWE Top 25

為了呼應新的關聯性，本版本也包含支援 2022 CWE Top 25 的新 Fortify Software Security Center 報告套件，您可以從 Fortify 客戶支援入口網站的 Premium Content 下方進行下載。

Fortify Taxonomy：軟體安全性錯誤

Fortify Taxonomy 網站包含了新增類別支援的說明，網址為：https://vulncat.fortify.com。客戶若在舊網站尋找最新的支援更新，可從 Fortify 支援入口網站取得該更新內容。

[4] 需要 WebInspect 21.2.0.117 或更高版本修補程式中提供的 OAST 功能。

連絡 Fortify 技術支援

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

連絡 SSR

Alexander M. Hoole
Software Security Research 資深經理
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
軟體安全性研究經理
CyberRes Fortify
peter.blay@microfocus.com