# Fortify 軟體安全性內容

## 2021 更新 3

## 2021 年 9 月 24 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、Fortify WebInspect 和 Fortify Application Defender) 增添動能的安全情報。現在，CyberRes Fortify 軟體安全性內容能夠跨 27 種程式設計語言支援 1,051 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，2021.3.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)，以及 Fortify Premium Content。

## CyberRes Fortify Secure Coding Rulepacks [Static Code Analyzer]

隨著此發佈，Fortify Secure Coding Rulepacks 能夠跨 27 種程式設計語言偵測 831 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：

### Golang 標準程式庫更新 (版本：1.16)

擴大對 Go 標準程式庫的支援。Go 是 Google 設計的靜態型別開放原始碼語言，旨在協助輕鬆組建簡單、可靠且高效率的軟體。Go 在語法上與 C 相似，但具有記憶體安全機制、記憶體回收及結構型別。此更新涵蓋標準程式庫命名空間，並支援以下新類別：

- Cookie Security：Missing SameSite Attribute
- Cookie Security：Overly Permissive SameSite Attribute
- Go Bad Practices：Leftover Debug Code
- Insecure Randomness：Hardcoded Seed
- Insecure Randomness：User-Controlled Seed
- Insecure Transport：Cipher Suite Downgrade
- Insecure Transport：Weak SSL Protocol
- Often Misused：Privilege Management
- Weak Cryptographic Signature

### Android 11 更新 (API 層級：30)

Android 平台是專為行動裝置設計的開放原始碼軟體堆疊。Android 的一個主要元件是 Java API Framework，用於向應用程式開發人員公開 Android 功能。此版本將弱點偵測擴大至以 Java 或 Kotlin 編寫，藉此利用 Android Java API Framework 的原生 Android 應用程式。使用者應可期望從 Android 應用程式建模和 API 涵蓋範圍的更新中獲得改進的結果。此版本還包括以下新的權限管理弱點類別，為不安全的 Android 權限提供指引：

- Privilege Management：Android Activity Recognition
- Privilege Management：Android Calendar
- Privilege Management：Android Call Log
- Privilege Management：Android Camera
- Privilege Management：Android Contacts
- Privilege Management：Android Microphone
- Privilege Management：Android Sensors

### iOS 標準程式庫更新 (版本：iOS 14)

此版本更新了我們對 Swift 和 Objective-C 的 iOS 14 程式庫 API 的支援。更新集中在以下框架上：

- UIKit
- UserNotification
- SwiftUI
- MessageUI

使用者應該會看到 Insecure IPC、Link Injection、Path Manipulation、Privacy Violation、Shoulder Surfing 和 System Information Leak 類別的改進。

### Micro Focus Visual COBOL 更新 (版本：7.0)

已擴大對 Micro Focus Visual COBOL 版本 7 的支援，藉此新增對以下兩種弱點類別的支援：

- Integer Overflow
- Race Condition：File System Access

### SAPUI5/OpenUI5 支援 [1] (版本：1.93)

SAPUI5 是由 SAP 設計的一種用戶端 JavaScript 架構，與開放原始碼的 OpenUI5 共用一組核心控制程式庫。此版本為識別以下類別的弱點提供初步支援：

- Cross-Site Scripting：DOM
- Cross-Site Scripting：SAPUI5 Control
- Cross-Site Scripting：Self
- Privacy Violation
- SAPUI5 Misconfiguration：Unsanitized Editor
- System Information Leak：External

### JSON 支援 [2]

JavaScript Object Notation (JSON) 是一種輕量級的資料交換格式。此版本為識別以下類別的 JSON 弱點提供了改進的支援：

- Password Management：Empty Password
- Password Management：Hardcoded Password
- Password Management：Null Password
- Password Management：Password in Comment[3]

### Kotlin 標準程式庫更新 (版本：1.4.30)

Kotlin 是一種通用的靜態類型語言，具有 Java 互通性。此版本包括對 Kotlin 1.4 中鎖定 Java 虛擬機器 (JVM) 引入的新標準程式庫 API 的更新支援。

---

[1] 使用 Static Code Analyzer v21.2.0 或更高版本時預期會得到改進的結果。

[2] 需要 Static Code Analyzer v21.1.0 和旗標：'-Dcom.fortify.sca.use.json-analyzer=true'。

[3] 需要 Static Code Analyzer v21.2.0 或更高版本。從 Static Code Analyzer v21.2.0 開始不需要旗標。

### ECMAScript 2021 (版本：ECMA-262)

支援 ECMAScript 2021 中引入的新 API。ECMAScript 是一種通用程式設計語言，由 ECMAScript 語言規格定義，以整合到所有現代網頁瀏覽器中而聞名。但是，它越來越普遍地用於建立網頁伺服器、行動應用程式和其他類型的傳統應用程式。在掃描目標鎖定最新 ECMAScript 標準的應用程式時，客戶應該期待改進的資料流。

### 2021 Common Weakness Enumeration (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。7 月發佈的 2021 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 2021 CWE Top 25 之間的關聯性。

### 其他勘誤

在此發佈中，我們持續盡可能投入一切資源，來確保我們可以降低誤報問題數，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問題的變更：

#### *不再支援 18.x 之前的 Static Code Analyzer 版本：*

正如在 2020.4 版本中觀察到的那樣，我們將繼續支援 Static Code Analyzer 的最後四個主要版本。因此，這將是支援 Static Code Analyzer 18.x 之前版本的最後 Rulepack 版本。在下一個版本中，Static Code Analyzer 18.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 Static Code Analyzer 的版本。

在下一個版本中，我們將繼續支援 Static Code Analyzer 的最後四個主要版本。

#### *Java J2EE 改進功能：*

已改進 *Privacy Violation* 和 *System Information Leak* 類別中 javax.servlet API 的支援。

#### *Android 繫結服務：*

隨著我們持續支援 Android，此版本涵蓋了 Android 繫結服務。客戶可能會遇到源自 Android 繫結服務方法參數的新資料流問題。在繫結服務中呼叫方法時，可能會引入重複的資料流子追蹤。

#### *Node.js 中的弱式密碼編譯雜湊：*

確定弱式密碼編譯雜湊是否用於 Node.js 應用程式中。

### *OWASP ASVS 4.0 對應關係現在包含對層級的支援*

為了支援客戶，使其能查詢違反特定 OWASP Application Security Verification Standard (ASVS) 應用程式安全驗證層級 (L1、L2 和 L3) 所舉報的問題，最新的安全性內容已將這些層級新增到對應名稱中。客戶現在可以在 *OWASP ASVS 4.0* 群組中搜尋相關的 *L1*、*L2* 和 *L3* 關鍵字，以及設計相關的篩選集合和篩選範本，以便在 AuditWorkbench 和 Software Security Center (SSC) 中使用。

### *誤報改進功能：*

我們在此版本中持續移除誤報。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：

- jQuery 程式碼中的 *Cross-Site Scripting* 誤報
- .NET 應用程式中使用 JsonIgnore 屬性的 *Privacy Violation：Shoulder Surfing*
- 在只能控制一個數字的 *Path Manipulation* 問題上更一致地降低 Fortify Priority Order
- 當密碼是列舉的一部分時，我們將不再識別 Swift 中的密碼
- .NET 中的 *Missing XML Validation* 問題
- Java 專案中的 *Missing Check against Null*

## CyberRes 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：HTTP Request Smuggling**

HTTP2 over clear text smuggling 或 h2c smuggling 是傳統 HTTP request smuggling 的替代方案，後者會濫用 h2c-unaware 前端 (例如 Proxy 伺服器) 來建立通往後端系統的通道。攻擊者可以使用此通道，將額外的要求偷傳到後端伺服器，而不被前端伺服器偵測到。如此一來，攻擊者就可能繞過前端的授權控制並存取後端系統上的管制資源。本版本包含的檢查可偵測會用於 h2c smuggling 攻擊的配置。

**Access Control：Missing Authorization Check**

GraphQL Introspection 能查詢伺服器以取得有關底層結構的資訊。Introspection 提供有關查詢、類型和欄位等元素的詳細資訊。GraphQL Introspection 通常預設為啟用。未經適當授權的攻擊者可能會濫用此資訊進行 SQL Injection 等攻擊和批次處理攻擊。此版本包含的檢查可偵測啟用了 introspection 的 GraphQL 端點。

**NoSQL Injection：MongoDB**

NoSQL script injection 弱點允許攻擊者在資料庫中注入惡意查詢。MongoDB 是 NoSQL 資料庫之一，其說明文件表示允許應用程式執行 JavaScript 操作。NoSQL Injection 非常危險，因為未經驗證的攻擊者可以擷取資料或執行 JavaScript 程式碼。此舉可能導致遠端程式碼執行、機密洩漏、應用程式資料完整性和 Denial of Service (DoS) 攻擊。此版本包含的檢查可偵測 MongoDB 中 NoSQL script injection。

**Dynamic Code Evaluation：Unsafe Deserialization**

7.0 之前的 ForgeRock AM 伺服器和 14.6.4 之前的 OpenAM 伺服器中的預先授權不安全 Java 還原序列化弱點已被 CVE-2021-35464 識別出來。此弱點允許攻擊者在 jato.pageSession 參數中製作惡意序列化物件，並透過單一要求將其傳送到端點「/ccversion/Version」。存在此弱點，是因為應用程式中使用了不安全的第三方 Java 程式庫。此問題通常允許攻擊者在伺服器上執行任意程式碼、濫用應用程式邏輯或 Denial of Service (DoS) 攻擊。此版本包含一項檢查，可用來偵測目標網頁伺服器上是否存在此弱點。

**Cross-Site Scripting：DOM[4]**

當動態產生的網頁顯示未正確驗證的使用者輸入內容 (例如登入資訊) 時，將會發生 Cross-Site Scripting，從而允許攻擊者將惡意指令碼嵌入到產生的頁面中，然後在檢視該頁面的任何使用者的電腦上執行該指令碼。在基於 Document Object Model (DOM) 的 XSS 情況下，惡意內容會作為 DOM 操作的一部分執行。如果執行成功，DOM Cross-Site Scripting 弱點就可被利用來操縱或竊取 Cookie、建立可能被誤認為是有效使用者的要求、破壞機密資訊或在使用者系統上執行惡意程式碼。此版本包含一項新檢查，可用於偵測用戶端 URI 片段上的 DOM XSS。

**Web Server Misconfiguration：Insecure Mapping Directives**

將 Nginx 配置為在網頁伺服器上執行 PHP 有時會主張將每個以 .php 結尾的 URI 傳遞給後端 PHP 解譯器 (例如 FastCGI)。如果請求的完整路徑沒有指向實際存在的檔案，具有這種不安全 PHP 配置的 Nginx 會將 URL 路徑中的資料夾視為要執行的目標檔案。這種錯誤配置會允許攻擊者在任何類型的檔案 (例如影像檔) 中執行任意 PHP 程式碼，前提是它可以上傳到網頁伺服器並被存取。此版本包含一項檢查，可用來偵測目標網頁伺服器上是否存在此弱點。

[4] 需要 WI v21.2.0 或更高版本。

### Integer Overflow

從 0.5.6 到 1.13.2 的 Nginx 版本容易受到由 CVE-2017-7529 識別的 integer overflow 弱點的攻擊。此問題存在於 Nginx 範圍篩選模組中，允許攻擊者透過傳送特製請求來取得潛在的敏感資訊。此版本包含一項檢查，可用來偵測目標網頁伺服器上是否存在 CVE-2017-7529 弱點。

## 合規報告

### *2021 Common Weakness Enumeration (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。7 月發佈的 2021 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。此 SecureBase 更新包含與這些 CWE 類別的對應關係。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

### CWE Top 25 2021

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 CWE Top 25 2021 相關的檢查而自訂的原則。

## 其他勘誤

在此發佈中，我們持續盡可能投入一切資源，來確保我們可以降低誤報問題數，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問題的變更：

#### *LDAP Injection*

此版本改進了 LDAP Injection 檢查功能，以減少誤報並提高其結果的準確性。

# CyberRes 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。

### 2021 CWE Top 25

為了呼應新的關聯性，本版本也包含支援 2021 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。

## CyberRes Fortify 分類法：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 CyberRes Fortify 支援入口網站取得該更新內容。

## 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**

Software Security Research 經理
CyberRes Fortify
peter.blay@microfocus.com