Fortify 軟體安全性內容

2023 更新 4
2023 年 12 月 15 日

關於 OpenText Fortify Software Security Research

Fortify Software Security Research 團隊將尖端研究成果轉變爲可爲 Fortify 產品組合 (包括 OpenText™ Fortify Static Code Analyzer (SCA) 和 OpenText™ Fortify WebInspect) 增添動能的安全情報。現在，Fortify 軟體安全性內容能夠跨 33 種以上的語言支援 1,657 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，2023.4.0 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 33 種以上的語言偵測 1,432 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：

已改進對 Python 的支援 (支援的版本：3.12)

Python 是一種功能強大的通用程式設計語言，具有動態型別和高效率的高階資料結構。該語言支援多種程式設計範式，包括結構化、物件導向和函數式程式設計。此發佈藉由擴大我們對 Python 標準程式庫 API 變更的支援，增加了對最新版 Python 的涵蓋範圍。針對以下模組更新了現有規則涵蓋範圍：

- os
- pathlib
- tomllib

已改進對 Django 的支援 (支援的版本：4.2)

Django 是一個使用 Python 編寫的 Web 架構，旨在促進安全、快速的 Web 開發。開發的速度和安全性是透過架構中的高度抽象化來實現的，其中使用程式碼建構與產生來大幅減少樣板程式碼。在此發佈中，我們更新了現有的 Django 涵蓋範圍以支援以下版本：4.0、4.1 和 4.2。

改進的涵蓋範圍包括以下命名空間：*asyncio*、*django.core.cache.backends.base.BaseCache*、*django.db.models.Model* 和 *django.middleware.security.SecurityMiddleware*。此外，我們也改進了弱點類別的涵蓋範圍，具體如下：

- Header Manipulation
- Insecure Cross-Origin Opener Policy
- Resource Injection
- Setting Manipulation

PyCryptodome 和 PyCrypto (支援的版本：3.19.0)

PyCryptodome 是一款獨立運作的 Python 套件，可提供豐富全面的加密演算法和通訊協定。該套件經過擴充，可做爲更積極維護的 PyCrypto 程式庫版本。PyCryptodome 專爲提供範圍廣泛的加密功能所設計，使其成爲開發人員在 Python 應用程式中實現安全通訊、資料保護及加密作業的多功能選擇。

弱點類別的初始涵蓋範圍包括如下：

- Key Management: Empty Encryption Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded Encryption Key
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Key Management: Unencrypted Private Key
- Password Management: Hardcoded Password
- Password Management: Lack of Key Derivation Function
- Password Management: Password in Comment
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Insufficient Key Size
- Weak Encryption: Stream Cipher
- Weak Encryption: User-Controlled Key Size

偵測源自機器學習 (ML) 和人工智慧 (AI) 模型的風險

隨著生成式 AI 和大型語言模型 (LLM) 的使用迅速改變軟體產業的解決方案空間，新的風險也隨之而起。初始 Fortify 支援涵蓋使用 OpenAI API、Amazon Web Services (AWS) SageMaker 或 LangChain 的 Python 專案。支援可偵測因對 AI/ML 模型 API 回應的隱含信任而導致的弱點，還可提供以下獨特功能：

對 Python OpenAI API 的初始支援 (支援的版本：1.3.8)

OpenAI Python 程式庫讓開發人員能夠輕鬆存取 OpenAI REST API，來與 GPT-4 和 DALL-E 等 OpenAI 模型進行互動。而 OpenAI API 可使應用程式傳送提示給 OpenAI 模型，並可接收產生的回應以及微調現有模型。OpenAI Python 模組支援的能力包括傳送和接收由 ***httpx*** 提供技術支援的非同步和同步請求。支援包括識別模型的潛在危險輸出以及以下新類別：

- Cross-Site Scripting: AI

對 Python AWS SageMaker (Boto3) 的初始支援 (支援的版本：1.33.9)

AWS SageMaker 是 Amazon AWS 龐大服務體系下的產品。AWS SageMaker 提供一系列廣泛的工具來支援各種 ML 專案，從訓練自訂模型到設定完全由 MLOps 提供支援的開發管道。Amazon 的 SDK for

Python (Boto3) 能夠與各種 AWS 產品/服務進行通訊，包括 AWS SageMaker。支援包括識別模型的潛在危險輸出以及以下新類別：

- Cross-Site Scripting: AI

對 Python LangChain 的初始支援 (支援的版本：0.0.338)[1]

LangChain 是一款主流的開放原始碼協調架構，用於開發使用大型語言模型 (LLM) 的應用程式。LangChain 提供的工具和 API 可讓您更輕鬆地建立 LLM 導向型應用程式，例如聊天機器人和虛擬客服。這些可以做爲以 Python 和 JavaScript 爲基礎的程式庫來使用。支援包括識別模型的潛在危險輸出、偵測 *Path Manipulation* 以及以下新類別：

- Cross-Site Scripting: AI

.NET 8 支援 (支援的版本：8.0.0)

.NET 8 是 .NET 7 的延續，是一個跨平台、免費、開放原始碼的開發架構，可讓程式設計師使用一組標準化的 API 以不同的語言 (例如 C# 和 VB) 編寫應用程式。此發佈擴大了對最新版本 .NET 的涵蓋範圍，以改進對新 API 和現有 API 的弱點偵測。

擴大的涵蓋範圍橫跨以下命名空間：

- System.Collections.Frozen
- System.Net.Http.Json
- System
- System.Security
- System.Text
- System.Text.Unicode
- System.Net.Http

Java Simplified Encryption (Jasypt) (支援的版本：1.9.3)

Java Simplified Encryption (Jasypt) 是一個小型 Java 程式庫，用於執行以密碼爲基礎的加密，以及建立儲存用的密碼摘要。該程式庫具有與主流 Java 架構 (例如 Spring、Wicket 和 Hibernate) 整合的功能。

弱點類別的初始涵蓋範圍包括如下：

- Insecure Randomness
- Key Management: Empty PBE Password
- Key Management: Hardcoded PBE Password
- Key Management: Null PBE Password
- Password Management: Lack of Key Derivation Function
- Privacy Violation: Heap Inspection

[1] LangChain 還不夠完善。在生產使用前，請務必審慎考量安全性。

- Setting Manipulation
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Mode of Operation

ECMAScript 2023

ECMAScript 2023 (也稱爲 ES2023 或 ES14)，是 JavaScript 語言的最新 ECMAScript 標準版本。ES2023 的主要功能包括新的陣列函數，允許藉由複製並從末尾搜尋來變更這些函數。對 ES2023 的支援，將所有相關 JavaScript 弱點類別的涵蓋範圍延伸到最新版本的 ECMAScript 標準。

Prototype Pollution

Prototype Pollution 是存在於 JavaScript 應用程式中的弱點，可讓惡意使用者略過或影響業務邏輯，同時可能執行自己的程式碼。

此 Rulepack 更新會偵測攻擊者可否在以下的 NPM 套件中汙染物件的原型：

- assign-deep
- deap
- deep-extend
- defaults-deep
- dot-prop
- hoek
- lodash
- merge
- merge-deep
- merge-objects
- merge-options
- merge-recursive
- mixin-deep
- object-path
- pathval

Kubernetes 組態

Kubernetes 是一種開放原始碼容器管理解決方案，用於自動部署、擴充及管理容器化應用程式。這款解決方案提供以容器爲中心的基礎架構抽象層，可消除對底層基礎架構的依賴，實現可攜式部署，並簡化複雜分散式系統的管理。改進的弱點類別涵蓋範圍包括如下：

- Kubernetes Misconfiguration: Improper API Server Network Access Control
- Kubernetes Misconfiguration: Improper CronJob Access Control
- Kubernetes Misconfiguration: Improper DaemonSet Access Control
- Kubernetes Misconfiguration: Improper Deployment Access Control
- Kubernetes Misconfiguration: Improper Job Access Control
- Kubernetes Misconfiguration: Improper Pod Access Control
- Kubernetes Misconfiguration: Improper RBAC Access Control
- Kubernetes Misconfiguration: Improper ReplicaSet Access Control
- Kubernetes Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Misconfiguration: Improper StatefulSet Access Control
- Kubernetes Misconfiguration: Insecure Secret Transport
- Kubernetes Misconfiguration: Insufficient Kubelet Logging
- Kubernetes Misconfiguration: Scheduler System Information Leak
- Kubernetes Misconfiguration: Uncontrolled Kubelet Resource Consumption
- Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control
- Kubernetes Terraform Misconfiguration: Improper Deployment Access Control
- Kubernetes Terraform Misconfiguration: Improper Job Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Network Access Control
- Kubernetes Terraform Misconfiguration: Improper RBAC Access Control
- Kubernetes Terraform Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control
- Kubernetes Terraform Misconfiguration: Insecure Secret Transport

DISA STIG 5.3

爲了在合規領域支援我們的聯盟客戶，已新增 Fortify Taxonomy 與 Defense Information Systems Agency (DISA) Application Security and Development STIG 5.3 版之間的關聯性。

OWASP Mobile Top 10 Risks 2023

Open Worldwide Application Security Project (OWASP) Mobile Top 10 Risks 2023 旨在提高人們對於行動安全風險的意識，並爲參與行動應用程式開發與維護的人員提供訓練。爲了向希望減輕 Web 應用程式風險的客戶提供支援，已新增 Fortify Taxonomy 與新發佈的 OWASP Mobile Top 10 2023 之間的關聯性。

其他勘誤

在此版本中，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 20.x 之前的 Fortify Static Code Analyzer 版本

如我們 2023.3 發佈公告中所述，這是支援 20.x 之前的 Static Code Analyzer 版本的最後 Rulepack 版本。在此發佈中，20.x 之前的 Static Code Analyzer 版本將不會載入 Rulepack。此時將會要求降

級 Rulepack 或升級 Static Code Analyzer 版本。在未來的發佈中，我們將繼續支援 Static Code Analyzer 的最後四個主要版本。

減少誤報及其他顯著的偵測改進事項

我們在此版本中持續著手移除誤報。客戶可望看到我們進一步移除誤報，以及與以下領域相關的其他顯著改進：

- *ASP.NET Misconfiguration: Persistent Authentication* – 已移除使用表單驗證服務的 ASP.NET 應用程式中的誤報
- *Credential Management: Hardcoded API Credentials* – 已移除 HTTP Bearer 權杖相關 Scret Sanning 中的誤報
- *Credential Management: Hardcoded API Credentials* – 偵測到 Avature API 金鑰的新問題
- *Cross-Site Request Forgery* – 在使用 `Express.js` JavaScript 架構的 NodeJS 應用程式中偵測到新問題
- *Cross-Site Scripting* – 在使用 `html/template` 套件的 Go 應用程式中偵測到新問題
- *Cross-Site Scripting: Reflected* – 已移除使用 `ListControl` 類別的 ASP.NET 應用程式中的誤報
- *Denial of Service: Format String* – 與 OWASP Top 10 類別的對應不正確
- *Insecure Transport* – 已移除 ASP.NET 應用程式中與處理私人使用者資料的控制器方法相關的誤報
- *Insecure Transport: Mail Transmission* – 已移除使用 `smtplib.SMTP` 類別的 Python 應用程式中的誤報
- *Key Management: Hardcoded Encryption Key* – 已移除使用 `RSAKeyGenParameterSpec` 類別的 Java 應用程式中的誤報
- *Link Injection: Missing Validation* – 已移除使用 `WKNavigationDelegate` 通訊協定[2] 的 Swift 和 Objective-C 應用程式中的誤報
- *Mass Assignment: Insecure Binder Configuration* – 已移除使用 Jakarta EE API 的 Java 應用程式中的誤報
- *Password Management: Password in Configuration File* – 已移除組態檔中的誤報
- *Path Manipulation* – 在 PHP 應用程式中偵測到檔案上傳的新問題
- *SQL Injection* – 在使用 marsdb 資料庫的 NodeJS 應用程式中偵測到新問題
- *SQL Injection: MyBatis Mapper* – 在 MyBatis 對應程式 XML 檔案中偵測到新問題
- *String Termination Error* – 已移除使用`printf()` 及其變體的 C/C++ 應用程式中的誤報
- *System Information Leak: Incomplete Servlet Error Handling* – 已移除 Java 應用程式中的誤報
- *Weak Encryption: Insecure Initialization Vector* – 已移除使用 `Pycryptodome` 程式庫的 Python 應用程式中的誤報
- *Unreleased Resource: Streams* – 已在使用 `java.nio.file` AP 的 Java 應用程式中識別出誤報
- Visualforce 應用程式中與使用者設定檔資訊相關的各種資料流程誤報

[2] 需要使用 Fortify Source Code Analyzer 23.1 或更高版本

類別名稱變更

當弱點類別名稱發生變更時，若將先前掃描與新掃描的分析結果合併，可能會導致類別的增加/移除。

爲了提高一致性，已重新命名以下兩種類別：

移除的類別	新增的類別
Azure ARM Misconfiguration: Insecure DataBricks Storage	Azure ARM Misconfiguration: Insecure Databricks Storage
Azure ARM Misconfiguration: Insecure Redis Enterprise Transport	Azure ARM Misconfiguration: Insecure Redis Transport

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

Access Control: 管理介面

此發佈包含一項檢查功能，可用於在閘道制動器端點啓用、遭到暴露且未受保護時偵測 Spring Cloud Gateway 的不安全組態。此情況下，攻擊者可以建立新路由並代表應用程式存取內部資產或敏感資產。這可能會導致雲端中繼資料金鑰被盜、內部應用程式暴露或 Denial Of Service (DoS) 攻擊。

Expression Language Injection: Spring

Spring Cloud Gateway 版本 3.1.0、3.0.0 至 3.0.6 以及 3.0.0 之前的版本都包含 CVE-2022-22947 所識別的安全弱點。當閘道致動器端點啓用、遭到暴露且未受保護時，此弱點會允許執行 Code Injection 攻擊。此發佈包含一項檢查功能，可用於偵測使用受影響 Spring Cloud Gateway 版本的目標伺服器上是否存在此弱點。

Insecure Deployment: Unpatched Application

TeamCity On-Premises 伺服器版本 2023.05.3 及更早版本容易遭受驗證略過攻擊，讓未經驗證的攻擊者能在伺服器上實現遠端程式碼執行 (RCE)。此弱點已由 CVE-2023-42793 所識別。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。

資訊探索：無文件記錄的 API

API 端點無文件記錄或僅提供有限文件，都可能爲攻擊者提供未充分測試安全弱點的攻擊面。攻擊者可能會執行偵察來探索已被取代、未修補和未維護的端點，從而獲得對敏感資訊或危險功能的存取權限。此發佈包含一項檢查功能，旨在探索可存取、但未在 API 規格文件中定義的版本化 API 端點。

合規報告

DISA STIG 5.3

爲了支援我們聯盟客戶的合規需求，本版本包含 WebInspect 檢查與最新版本 Defense Information Systems Agency Application Security and Development (DISA) STIG 5.3 版之間的關聯性。

原則更新

DISA STIG 5.3

在 WebInspect SecureBase 支援的原則清單中，已新增爲納入與 DISA STIG 5.3 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領域相關回報結果的變更。

Insecure Transport: SSLv3/TLS Renegotiation Stream

TLS 1.3 不支援重新交涉。此發佈改進了 Renegotiation Stream Injection 檢查功能，以減少誤報並提高結果的準確性。

HTML5: Cross-Site Scripting Protection

X-XSS-Protection 標頭在所有現代瀏覽器中均已被取代。在此發佈中，我們已取代遺失或設定有誤的 X-XSS-Protection 標頭檢查。

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。

DISA STIG 5.3 和 OWASP Mobile Top 10 2023

爲了呼應新的關聯性，此發佈也包含支援 DISA STIG 5.3 和 OWASP Mobile Top 10 2023 的全新 OpenText™ 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，網址爲：https://vulncat.fortify.com。

聯絡 Fortify 客戶支援

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

連絡 SSR

Alexander M. Hoole
Software Security Research 資深經理
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Software Security Research 經理
OpenText Fortify
pblay@opentext.com
+1 (669) 309-1634