Software Security Research 發佈公告

Fortify 軟體安全性內容

2022 更新 2

2022 年 6 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 (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 1,220 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，2022.2.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)，以及 Fortify Premium Content。

Fortify Secure Coding Rulepacks [SCA]

隨著此發佈，Fortify Secure Coding Rulepacks 能夠跨 30 種程式設計語言偵測 1,000 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：

.NET 改進 (支援的版本：6.0)

.NET 是一般的程式設計平台，它讓程式設計師能使用 C# 和 VB.NET 等語言搭配一組標準化的 API 來撰寫程式碼。此版本將我們的涵蓋範圍擴大到最新版本的 .NET 以改善資料流程，同時也擴充了以下類別的 API 涵蓋範圍：

- Access Control: Database
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- SQL Injection
- System Information Leak: External
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Encryption: Insecure Mode of Operation

ASP.NET Core 改進 (支援的版本：6.0)

ASP.NET Core 是搭配 .NET 使用的旗艦 Web 架構。此架構包括建立多種類型應用程式 (包括 MVC Web 應用程式和 Web API) 的功能。此版本將我們的涵蓋範圍擴大到最新版本的 ASP.NET Core，包括最少的 API，同時也擴充了我們支援的類別，包括：

- .NET Attribute Misuse: Authorization Bypass
- ASP.NET Bad Practices: Compression Over Encrypted WebSocket Connection
- ASP.NET Middleware Out of Order: Default Cookie Configuration
- ASP.NET Middleware Out of Order: Insecure Transport
- ASP.NET Middleware Out of Order: Insufficient Logging
- ASP.NET Misconfiguration: Insecure Transport
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute

Weak Cryptographic Implementation

Psychic Signatures (CVE-2022-21449) 是 Java 實作橢圓曲線數位簽章演算法 (ECDSA) 過程中的一個弱點。此弱點會允許攻擊者強制應用程式接受全零的數位簽章為有效。易受攻擊的 Java 版本包括：15、16、17 和 18。如果使用易受攻擊的 Java 版本，攻擊者可以偽造某些類型的 SSL 憑證、簽名的 JSON Web 權杖，甚至是 WebAuthn 驗證訊息。此版本新增了對在 Java 中報告 *Weak Cryptographic Implementation* 的支援。

Jakarta EE 支援 (支援的版本： 9.0.0)

Jakarta EE 提供所有廠商均適用的全方位開放型規格集，採用開放原始碼架構的形式，可用於開發雲端原生 Java 應用程式。它原稱為 Java EE (或 J2EE)，是最知名的伺服器端 Java 架構之一。此版本新增了對現有 Java EE 涵蓋範圍的改進，橫跨 52 個弱點類別。

Secret Scanning 改進

Secret Scanning 是一種在原始碼和組態檔案中搜尋及偵測密碼的技術。有時，包含密碼或 API 權杖的組態檔案可能會意外洩露到原始碼儲存庫。此版本納入對常見密碼雜湊格式的支援。涵蓋範圍包括識別常見密碼雜湊格式和產品組態檔案中的密碼，包括以下內容：OpenVPN、Windows 遠端桌面、netrc、IntelliJ IDEA、DBeaver、FileZilla、Heroku 和 DigitalOcean doctl。
針對以下類別提供了增強的涵蓋範圍：

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Password Management: Hardcoded Password
- Password Management: Password in Configuration File
- Password Management: Weak Cryptography

Express JS 改進 (支援的版本： 4.x)[1]

Express 是一個使用 Node.js 組建 Web 應用程式的架構。它提供路由、錯誤處理、範本化、中介軟體管理和 HTTP 相關公用程式的功能。
在此版本中，我們已改進對以下類別的 Express 4.x 的支援：

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Insecure Transport
- Path Manipulation
- Privacy Violation
- Process Control
- Setting Manipulation
- System Information Leak: External

JavaScript Handlebars (支援的版本：4.7.7)

Handlebars 是一個 JavaScript 程式庫，旨在製作可重複使用的 Web 範本。這些範本由 HTML、文字和運算式組成。運算式會直接嵌入 HTML 程式碼中，並作為預留位置供程式碼插入內容，從而使文件易於重複使用。

---

[1] 需要 SCA 版本 22.1.1

在此版本中，我們已新增對 Handlebars 4.7.7 的支援，改進了資料流程涵蓋範圍，並且擴充了以下類別的 API 涵蓋範圍：

- Cross-Site Scripting: Handlebars Helper
- Handlebars Misconfiguration: Escaping Disabled
- Handlebars Misconfiguration: Prototypes Allowed
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak
- Template Injection

JavaScript Mustache (支援的版本：4.2.0)

Mustache 是一個開放原始碼的無邏輯範本系統，它提供範本和視圖作為建立動態範本的基礎。範本包含呈現格式和程式碼，而視圖則包含要納入範本的資料。
在此版本中，我們已新增對 Mustache 4.2.0 的支援，以識別 *Template Injection* 弱點。

GraphQL.js (支援的版本：16.5.0)

GraphQL.js 是 GraphQL 的 JavaScript 參考實作，廣泛用於 JavaScript 應用程式。此版本新增了初始 GraphQL 伺服器支援，以偵測下列存在於 GraphQL API 中的弱點類別：

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

Graphene-Python (支援的版本：3.0.0)

Python-Graphene 是適用於 Python 應用程式的熱門 GraphQL 伺服器架構。此版本改進了我們從 2022.1.0 開始的 GraphQL 伺服器支援，以偵測下列存在於 GraphQL API 中的弱點類別：

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

雲端基礎架構即程式碼

基礎架構即程式碼 (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。此版本新增了對 IaC 的擴大支援。支援的技術包括用於部署到 Azure 和 AWS 的 Ansible 組態，以及用於部署到 Azure 和 GCP 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。

Terraform 組態：

Terraform 是一種開放原始碼基礎架構即程式碼工具，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 ***Microsoft Azure*** 基礎架構的設定及管理。在此版本中，我們報告了有關 Microsoft Azure 服務 Terraform 組態的以下類別：

- Azure Terraform Misconfiguration: Insecure App Service Transport
- Azure Terraform Misconfiguration: Insecure CDN Endpoint Transport
- Azure Terraform Misconfiguration: Insecure Function App Transport
- Azure Terraform Misconfiguration: Insecure Logic App Transport
- Azure Terraform Misconfiguration: Insecure MariaDB Transport
- Azure Terraform Misconfiguration: Insecure MySQL Transport
- Azure Terraform Misconfiguration: Insecure Network Monitor Transport
- Azure Terraform Misconfiguration: Insecure PostgresSQL Transport
- Azure Terraform Misconfiguration: Insecure Redis Cache Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Redis Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Transport
- Azure Terraform Misconfiguration: Insecure Storage Account Transport

Terraform 提供者可支援 ***Google Cloud Platform (GCP)*** 基礎架構的設定和管理。在此版本中，我們報告了有關 Google Cloud Platform Terraform 組態的以下類別：

- GCP Terraform Bad Practice: Overly Permissive Service Account
- GCP Terraform Misconfiguration: BigQuery Dataset Publicly Accessible
- GCP Terraform Misconfiguration: Cloud DNS DNSSEC Disabled
- GCP Terraform Misconfiguration: Cloud KMS CryptoKey Publicly Accessible
- GCP Terraform Misconfiguration: Cloud SQL Backup Disabled
- GCP Terraform Misconfiguration: Cloud Storage Bucket Publicly Accessible
- GCP Terraform Misconfiguration: Compute Engine Access Control
- GCP Terraform Misconfiguration: Compute Engine Default Service Account
- GCP Terraform Misconfiguration: Compute Engine Project-Wide SSH
- GCP Terraform Misconfiguration: Google Project Network Access Control
- GCP Terraform Misconfiguration: Insecure Cloud SQL Transport
- GCP Terraform Misconfiguration: Insecure Load Balancer Transport
- GCP Terraform Misconfiguration: Insufficient Cloud Storage Bucket Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Monitoring
- GCP Terraform Misconfiguration: Insufficient VPC Flow Logging
- GCP Terraform Misconfiguration: GKE Cluster Administrative Interface Access Control
- GCP Terraform Misconfiguration: GKE Cluster Certificate-Based Authentication
- GCP Terraform Misconfiguration: GKE Cluster Legacy Authorization
- GCP Terraform Misconfiguration: GKE Cluster HTTP Basic Authentication
- GCP Terraform Misconfiguration: GKE Container-Optimized OS Not In Use
- GCP Terraform Misconfiguration: GKE Node Auto-Upgrade Disabled

- GCP Terraform Misconfiguration: Weak Cryptographic Cloud DNS Signature
- GCP Terraform Misconfiguration: Weak GKE Cluster Network Management
- GCP Terraform Misconfiguration: Weak Key Management

Ansible 組態：
Ansible 是一個開放原始碼自動化工具，可為各種環境提供組態管理、應用程式部署、雲端佈建和節點協調。

Ansible 包含支援設定及管理 ***Amazon Web Services (AWS)*** 的模組。在此版本中，我們報告了有關 AWS Ansible 組態的以下類別：

- AWS Ansible Misconfiguration: Amazon RDS Publicly Accessible
- AWS Ansible Misconfiguration: Insecure CloudFront Distribution Transport
- AWS Ansible Misconfiguration: Insufficient CloudTrail Logging

Ansible 還包括支援設定及管理 ***Microsoft Azure 雲端運算服務*** 的模組。在此版本中，我們報告了有關 Microsoft Azure Ansible 組態的以下類別：

- Azure Ansible Misconfiguration: Overly Permissive Azure SQL Database Firewall

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：

Log4j (支援的版本：2.17)

對 Log4j 的支援現在包括偵測新類別 *Denial of Service: Stack Exhaustion*。

Oslo.config (支援的版本：8.8.0)

對 Python 的 oslo.config 的初始支援包括偵測新類別 *Privacy Violation: Unobfuscated Logging*。

Objective-C 錯誤修正和效能改進

客戶使用 2022R1 Rulepacks 掃描包含 Objective-C 檔案的專案時，可能會遇到以下問題：

- 在掃描階段，「[error] Unexpected exception during dataflow analysis...」形式的錯誤訊息可能會出現在 SCA 輸出或記錄檔中
- 資料流程分析中的掃描時間異常地久，可能導致喪失資料流程的問題

已將 Objective-C Hotfix Rulepack 提供給受影響的客戶來解決這些問題。此官方 R2 版本中包含相同的修正程式。使用 Hotfix Rulepack 的客戶應在更新到 R2 版本 Rulepack 之後立即移除 Hotfix Rulepack。

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：

- *SQL Injection: iBatis Data Map* - 在遇到常值「$」字元時防止誤報
- *Password Management: Password in Configuration File* - 當值是變數預留位置時防止誤報
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property* - 使用 [BindRequired] 屬性時，在 C# ASP.NET 應用程式中防止誤報
- *Often Misused: Authentication* - 減少 Java 應用程式中的誤報
- *XSS: Content Sniffing* - 減少 Java Spring 應用程式中的誤報
- *Privacy Violation* - 減少 .NET 應用程式中的誤報
- *SOQL Injection* 和 *SOSL Injection* - 現在，語義分析器所發現的問題會以 Fortify 優先順序為「低」來報告

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

OGNL Expression Injection: Double Evaluation

由 CVE-2022-26134 識別出的一個嚴重 OGNL Expression Injection 弱點會影響 Atlassian Confluence Server 和資料中心。此弱點會允許未經驗證的攻擊者在容易遭受攻擊的應用程式上執行任意程式碼。受影響的 Confluence Server 和 Data Center 版本為 1.3.0 到 7.4.16、7.13.0 到 7.13.6、7.14.0 到 7.14.2、7.15.0 到 7.15.1、7.16.0 到 7.16.3、7.17.0 到 7.17.3 以及 7.18.0。此版本包含一項檢查功能，可用來偵測受影響的 Confluence and Data Center 伺服器中是否存在此弱點。

Dynamic Code Evaluation: Code Injection

已發現 Spring Framework by Pivotal 容易受到 CVE-2022-22965 所識別出的遠端程式碼執行 (RCE) 弱點攻擊。遠端攻擊者可提供精心製作的要求參數，可能導致執行任意程式碼。此版本包含一項檢查功能，可用於偵測使用受影響 Spring Framework 版本的 Web 應用程式中是否存在此弱點。

Insecure Deployment: OpenSSL

OpenSSL 是一種廣泛用於支援 SSL/TLS 連線的熱門加密程式庫，其已被發現容易受到 CVE-2022-0778 所識別出的 Denial Of Service (DoS) 弱點攻擊。透過製作具有無效明確橢圓曲線參數的憑證，可以在受影響的系統上觸發無限迴圈 DoS。此版本包含一項檢查功能，可用於偵測目標 Web 伺服器上是否存在 CVE-2022-0778 弱點。由於此檢查有可能在受影響的系統上導致 DoS 條件，進而造成其無法提供服務，因此這項檢查並未納入標準原則中。請使用「所有檢查」(All Checks) 原則、自訂現有原則以納入這項檢查，或建立自訂原則來執行這項檢查。

其他勘誤

在此版本中，我們持續盡可能投入一切資源，以降低誤報數，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：

Password Management: Weak Password Policy

此版本包括對密碼原則檢查的小幅度改進，當輸入類型為文字方塊時，密碼/使用者名稱欄位的辨識準確度已提高。

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。

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。

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