Software Security Research 發佈公告

Fortify 軟體安全性內容

2022 更新 4

2022 年 12 月 16 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 1,286 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，2022.4.0 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 30 種程式設計語言偵測 1,066 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：

Flask 更新 (支援的版本：v2.2.x)

Flask 是一種以 Python 編寫而成的微型 Web 架構，不需要立即可用的一組特定工具或程式庫。它是輕量型且建立完善的架構，通常最適合中小型專案，但也能處理相對複雜的專案，例如小型 API 和微服務。支援的類別包括：

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- JSON Injection
- Often Misused: File Upload
- Open Redirect
- Path Manipulation
- Privacy Violation
- Server-Side Template Injection
- System Information Leak: External
- System Information Leak: Internal

Swift 的 iOS SDK 更新 (支援的版本： 16)[1]

Apple 的 iOS SDK 提供一系列的架構，讓開發人員能打造適用於 Apple iPhone 和 iPad 裝置的行動應用程式。此版本包含我們對 Swift 的 iOS SDK 支援的累加式更新。新增的規則和更新的規則都延伸了 Swift iOS 和 iPadOS 應用程式適用的 iOS SDK 15 和 16 中，我們的 Foundation 架構 API 涵蓋範圍。這些更新改進了許多現有弱點類別的問題偵測，包括：

- Insecure SSL: Overly Broad Certificate Trust
- Insecure Transport: Weak SSL Protocol
- Privacy Violation
- Resource Injection
- System Information Leak

[1] iOS SDK 16 的新規則要求使用 Fortify Static Code Analyzer 22.2 或更高版本。

Salesforce Apex 和 Visualforce 更新 (支援的版本：v55)[2]

Salesforce Apex 是用於建立 Salesforce 應用程式 (例如商業交易、資料庫管理、Web 服務和 Visualforce 頁面) 的程式設計語言。此更新改進了我們對 Database 作業、SOAP Web 服務、REST Web 服務、核心 Apex 系統 API、Crypto API 和 Visualforce 頁面元件的支援。Apex 新支援的類別包括：

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Permissive SameSite Attribute
- Cookie Security: Persistent Cookie
- Header Manipulation
- Header Manipulation: Cookies
- Insecure Transport
- Key Management: Hardcoded Encryption Key
- Log Forging (debug)
- Open Redirect
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Path Manipulation
- Privacy Violation
- Server-Site Request Forgery
- System Information Leak: External
- System Information Leak: Internal
- Weak Cryptographic Hash
- Weak Encryption: Insecure Initialization Vector

此外，以下支援的類別也做了其他改進：

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected

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。SSR 已支援多種類型的 Secret，SCA 會將 Secret Scanning 規則套用於所有**檔案類型**，**藉此允許尋找特定的** Secret，而不管程式碼語言為何。支援已延伸至涵蓋以下 Secret：

- Credential Management: Hardcoded API Credential，適用於硬式編碼的不記名權杖
- Password Management: Hardcoded Password，適用於 SQL 伺服器連線字串中的硬式編碼密碼
- Password Management: Password in Comment，適用於 XML 註解中的密碼 [3]

---

[2] 需要 Fortify Static Code Analyzer 22.2 或更高版本。
[3] 需要 Fortify Static Code Analyzer 22.2 或更高版本。

Google Guava 初始涵蓋範圍 (支援的版本：v31.1)

Guava 是一組來自 Google 的 Java 程式庫，其中包括新的集合類型 (例如 multimap 和 multiset)、不可變集合、圖形庫，以及用於並行、I/O、雜湊快取、基元、字串等的公用程式。它廣泛用於 Google 和其他公司的 Java 專案。支援的類別包括：

- Null Dereference
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- Unreleased Resource
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: User-Controlled Minimum Bits
- Weak Cryptographic Hash: User-Controlled Seed
- Weak Encryption

Hot Chocolate 初始涵蓋範圍 (支援的版本：12.15.2)

Hot Chocolate 是建置在 Microsoft .NET 平台之上的開放原始碼 GraphQL 伺服器。Hot Chocolate 讓開發人員能為其應用程式快速建立及部署以 GraphQL 為基礎的 API。此版本增加了對 Hot Chocolate 的初始支援，包括在使用 Hot Chocolate 開發的 GraphQL API 中偵測下列弱點類別：

- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- Privacy Violation
- System Information Leak: External
- Trust Boundary Violation

Java 的 gRPC 擴充和 Python 的初始涵蓋範圍 (支援的版本：1.49.1)

Google Remote Procedure Call (gRPC) 是一種多環境、多語言的現代開放原始碼高效能 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。

已擴充對 Java gRPC 的支援以涵蓋下列額外類別：

- Access Control: gRPC Authentication Bypass
- Insecure SSL: Overly Broad Certificate Trust
- Log Forging
- Setting Manipulation
- Unreleased Resource: Streams

已建立對 Python gRPC 的支援以涵蓋下列類別：

- Insecure Transport
- Insecure Transport: gRPC Channel Credentials
- Insecure Transport: gRPC Server Credentials
- Privacy Violation
- System Information Leak: External

雲端基礎架構即程式碼 (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。改進後的支援包括用於部署到 AWS、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。

Amazon AWS 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 Amazon Web Services (AWS) 基礎架構的設定及管理。在此版本中，我們報告了有關 Terraform 組態的以下類別：

- AWS Terraform Misconfiguration: Amazon API Gateway Publicly Accessible
- AWS Terraform Misconfiguration: Amazon EBS Insecure Storage
- AWS Terraform Misconfiguration: Amazon ElastiCache Insecure Transport
- AWS Terraform Misconfiguration: Amazon MQ Publicly Accessible
- AWS Terraform Misconfiguration: Amazon Neptune Publicly Accessible
- AWS Terraform Misconfiguration: Amazon RDS Insecure Storage
- AWS Terraform Misconfiguration: Amazon RDS Proxy Insecure Transport
- AWS Terraform Misconfiguration: Amazon RDS Publicly Accessible
- AWS Terraform Misconfiguration: Amazon Redshift Publicly Accessible
- AWS Terraform Misconfiguration: Amazon SNS Insecure Storage

Microsoft Azure 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 Terraform 組態的以下類別：

- Azure Terraform Bad Practices: AKS Cluster Missing Host-Based Encryption
- Azure Terraform Bad Practices: Azure Disk Snapshot Missing Customer-Managed Key
- Azure Terraform Bad Practices: Azure MySQL Server Missing Infrastructure Encryption
- Azure Terraform Bad Practices: Azure PostgreSQL Server Missing Infrastructure Encryption
- Azure Terraform Bad Practices: Container Registry Missing Customer-Managed Key
- Azure Terraform Bad Practices: Cosmos DB Missing Customer-Managed Key
- Azure Terraform Bad Practices: Missing Azure Storage Infrastructure Encryption
- Azure Terraform Bad Practices: Missing SQL Database Backup Encryption
- Azure Terraform Bad Practices: Scale Set Missing Host-Based Encryption
- Azure Terraform Bad Practices: Shared Image Missing Customer-Managed Key
- Azure Terraform Bad Practices: SQL Database Missing Customer-Managed Key

- Azure Terraform Bad Practices: Storage Account Missing Customer-Managed Key
- Azure Terraform Bad Practices: Storage Encryption Scope Missing Customer-Managed Key
- Azure Terraform Bad Practices: VM Missing Host-Based Encryption
- Azure Terraform Misconfiguration: AKS Cluster Missing Customer-Managed Key
- Azure Terraform Misconfiguration: Managed Disk Missing Customer-Managed Key
- Azure Terraform Misconfiguration: Missing SQL Database Encryption
- Azure Terraform Misconfiguration: VM Storage Missing Customer-Managed Key

Google Cloud Platform (GCP) 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 Google Cloud Platform 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 組態的以下弱點類別：

- GCP Terraform Bad Practices: Apigee Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: BigQuery Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: Cloud Bigtable Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: Cloud Functions Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: Cloud Spanner Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: Filestore Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: Pub/Sub Missing Customer-Managed Encryption Key
- GCP Terraform Bad Practices: Secret Manager Missing Customer-Managed Encryption Key
- GCP Terraform Misconfiguration: Compute Engine Missing Confidential Computing Features
- GCP Terraform Misconfiguration: Edge Cache Service Missing HTTP-to-HTTPS Redirect
- GCP Terraform Misconfiguration: Insecure App Engine Domain Transport
- GCP Terraform Misconfiguration: Insecure App Engine Transport
- GCP Terraform Misconfiguration: Insecure Cloud Function HTTP Trigger Transport
- GCP Terraform Misconfiguration: Insecure Edge Cache Service Transport
- GCP Terraform Misconfiguration: Insecure Supply Chain
- GCP Terraform Misconfiguration: URL Map Missing HTTP-to-HTTPS Redirect

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：

如我們 2022.3 發**佈公告中所述**[連結至 R3 發**佈公告**]，這是支援 19.x 之前的 Fortify Static Code Analyzer 版本的最後 Rulepack 版本。對於此本版本，19.x 之前的 Fortify Static Code Analyzer 版本將不會載入 2022.4 Rulepack。此時將會要求降級 Rulepack 或升級 Static Code Analyzer 至 19.x 或更高版本。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。

針對弱點類別修改 Fortify 優先順序中繼資料

讓我們的使用者能有效率地解決問題非常重要，因此我們不斷在 Fortify Priority Order 模型中研究更客觀的機制，以正確判斷問題分類。如 2022 R3 發**佈公告** [連結至 R3 發**佈公告**] 中所提到的這項工作，我們已著手開始檢閱我們所有規則涵蓋的類別，並確定了一些需要更新的領域。以下 96 個類別所關聯的 Fortify Priority Order 中繼資料已變更，因此**您可能會看到問題出現在相同或較低嚴重性的分類桶**中 (例如重大、高、中、低)。由於 Fortify Priority Order 值及其個別元件的變更，現有篩選可能會導致隱藏其他問題。

- Android Bad Practices: Encryption Secret Held in Static Field
- Android Bad Practices: Use of Released Camera Resource
- Android Bad Practices: Use of Released Media Resource
- Android Bad Practices: Use of Released SQLite Resource
- ASP.NET Bad Practices: Non-Serializable Object Stored in Session
- Buffer Overflow
- Buffer Overflow: Signed Comparison
- Code Correctness: Arithmetic Operation on Boolean
- Code Correctness: Function Not Invoked
- Code Correctness: Incorrect Serializable Method Signature
- Code Correctness: Memory Free on Stack Variable
- Code Correctness: Negative Content-Length
- Code Correctness: Premature Thread Termination
- Code Correctness: readObject() Invokes Overridable Function
- Code Correctness: Readonly Collection Reference
- ColdFusion Bad Practices: Unauthorized Include
- Cookie Security: Cookie not Sent Over SSL
- Cross-Site Scripting: Handlebars Helper
- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Reflected
- Cross-Site Scripting: Untrusted HTML Downloads
- Dangerous Method
- Denial of Service
- Denial of Service: Parse Double
- Denial of Service: Regular Expression
- Denial of Service: Stack Exhaustion
- Denial of Service: StringBuilder
- Double Free
- Dynamic Code Evaluation: Code Injection
- Dynamic Code Evaluation: Script Injection
- File Disclosure: Django
- File Disclosure: J2EE
- File Disclosure: Spring
- File Disclosure: Spring Webflow
- File Disclosure: Struts
- Format String: Argument Number Mismatch

- Header Manipulation: Cookies
- Header Manipulation: SMTP
- J2EE Bad Practices: Non-Serializable Object Stored in Session
- Log Forging
- Null Dereference[4]
- Often Misused: Authentication
- Often Misused: Boolean.getBoolean()
- Path Manipulation: Base Path Overwriting
- Path Manipulation: Zip Entry Overwrite
- Portability Flaw: File Separator
- Portability Flaw: Locale Dependent Comparison
- Privacy Violation
- Privacy Violation: Android Internal Storage
- Privacy Violation: BREACH
- Privacy Violation: Heap Inspection
- Privacy Violation: HTTP GET
- Privacy Violation: Image
- Privacy Violation: Keyboard Caching
- Privacy Violation: Screen Caching
- Privacy Violation: Sensitive Data Accessible From iTunes
- Privacy Violation: Shoulder Surfing
- Privacy Violation: Unobfuscated Logging
- Privilege Management: Android Disable
- Privilege Management: Missing API Permission
- Privilege Management: Missing Content Provider Permission
- Privilege Management: Missing Intent Permission
- Process Control
- Query String Injection: Android Provider
- Race Condition: PHP Design Flaw
- Race Condition: Singleton Member Field
- Race Condition: Static Database Connection
- SOQL Injection
- SOSL Injection
- System Information Leak: Overly Broad SQL Logging
- System Information Leak: PHP Errors
- System Information Leak: PHP Version
- Unreleased Resource: Cursor Snarfing
- Unsafe JNI
- Unsafe JSNI
- Unsafe Mobile Code: Access Violation

[4] Null Dereference 變更僅適用於 Java 和 .NET。

- Unsafe Mobile Code: Database Access
- Unsafe Native Invoke
- Use After Free
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Insufficient Key Size
- Weak Encryption: Missing Required Step
- Weak Encryption: User-Controlled Key Size
- Weak XML Schema: Lax Processing
- Weak XML Schema: Type Any
- Weak XML Schema: Unbounded Occurrences
- Weak XML Schema: Undefined Namespace

React Bad Practices: Dangerously Set InnerHTML

現在，若在 React 應用程式中使用「dangerouslySetInnerHTML」，將會標記為不良做法。

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：

- *Access Control: Database* – 在 Apex 中已移除輸入是來自**另一個資料庫呼叫時的問題**
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property* – 已減少當使用會強制執行資料某些特**徵的屬性時的誤報**
- *Dockerfile Misconfiguration: Dependency Confusion* – 已減少透過從頭開始延伸方式建立最小影像時的誤報
- *GraphQL Bad Practices: Introspection Enabled* – 已減少註冊以類別為基礎的 Flask 檢視時 Flask 應用程式中的誤報
- *Dynamic Code Evaluation: JNDI Reference Injection* – 已減少 Spring Boot 專案將「log4j2.version」Maven 屬性設為不受 Log4Shell 影響的某個版本時的誤報
- *Memory Leak* – 已減少使用 std::unique_ptr 時的誤報
- *Mass Assignment: Insecure Binder Configuration* – 已減少將 JSONConverter 註解與 DataContract、DataMember 或 IgnoreDataMember 搭配使用時的誤報
- *Privacy Violation* – 已減少有關 .NET 中列舉值的誤報
- *SQL Injection* – 已減少在 MyBatis 查詢註解中使用包含「$.」的已備妥陳述式時的誤報
- *Unreleased Resource* – 已減少配套某個集合中的資源時 C/C++ 掃描作業的誤報

PHP Misconfiguration: magic_quotes 類別已移除

以下三個弱點類別已移除，因為這些類別在支援的 PHP 版本中不再相關：

- PHP Misconfiguration: magic_quotes_gpc Enabled
- PHP Misconfiguration: magic_quotes_runtime Enabled
- PHP Misconfiguration: magic_quotes_sybase Enabled

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。

- *Code Correctness: Class Does Not Implement equals* 現在會回報為 *Code Correctness: Class Does Not Implement Equivalence Method*
- *Code Correctness: Class Does Not Implement Equals* 現在會回報為 *Code Correctness: Class Does Not Implement Equivalence Method*
- *Code Correctness: toString on Array* 現在會回報為 *Code Correctness: ToString on Array*
- *Code Correctness: null Argument to equals()* 現在會回報為 *Code Correctness: null Argument To Equivalence Method*
- *Code Correctness: null Argument to Equals()* 現在會回報為 *Code Correctness: null Argument To Equivalence Method*

此外，為了提高一致性，我們也重新修改了最近 IaC 支援中的以下 24 個類別。

- *Access Control: Azure Container Registry* 現在會回報為 *Azure ARM Misconfiguration: Improper Container Registry Network Access Control*
- *Access Control: Azure SQL Database* 現在會回報為 *Azure ARM Misconfiguration: Improper SQL Server Network Access Control*
- *Access Control: Cosmos DB* 現在會回報為 *Azure ARM Misconfiguration: Improper DocumentDB Network Access Control*
- *Access Control: Kubernetes Admission Controller* 現在會回報為 *Kubernetes Bad Practices: Improper Admission Controller Access Control*
- *Access Control: Kubernetes Image Authorization Bypass* 現在會回報為 *Kubernetes Misconfiguration: Image Authorization Bypass*
- *Ansible Bad Practices: CloudWatch Log Group Retention Unspecified* 現在會回報為 *AWS Ansible Misconfiguration: Insufficient CloudWatch Logging*
- *Ansible Bad Practices: Redshift Publicly Accessible* 現在會回報為 *AWS Ansible Misconfiguration: Improper Redshift Network Access Control*
- *Ansible Bad Practices: Unrestricted AWS Lambda Principal* 現在會回報為 *AWS Ansible Misconfiguration: Improper Lambda Access Control Policy*
- *Ansible Bad Practices: User-Bound AWS IAM Policy* 現在會回報為 *AWS Ansible Bad Practices: Improper IAM Access Control Policy*
- *Ansible Misconfiguration: Azure Monitor Missing Administrative Events* 現在會回報為 *Azure Ansible Misconfiguration: Insufficient Azure Monitor Logging*
- Azure Resource Manager Bad Practices: *Cross-Tenant Replication* 現在會回報為 *Azure ARM Misconfiguration:* Improper Storage Account Network Access Control
- *Azure Resource Manager Bad Practices: Remote Debugging Enabled* 現在會回報為 *Azure ARM Misconfiguration: Improper App Service Access Control*
- *Azure Resource Manager Bad Practices: SSH Password Authentication* 現在會回報為 *Azure ARM Misconfiguration: Improper Compute VM Access Control*
- *Azure Resource Manager Misconfiguration: Insecure Transport* 現在會回報為 *Azure ARM Misconfiguration: Insecure App Service Transport*
- *Azure Resource Manager Misconfiguration: Overly Permissive CORS Policy* 現在會回報為 *Azure ARM Misconfiguration: Improper CORS Policy*
- *Azure Resource Manager Misconfiguration: Security Alert Disabled* 現在會回報為 *Azure ARM Misconfiguration: Insufficient Microsoft Defender Monitoring*

- *Azure SQL Database Misconfiguration: Insufficient Logging* 現在會回報為 *Azure ARM Misconfiguration: Insufficient SQL Server Monitoring*
- *Insecure Storage: Missing EC2 AMI Encryption* 現在會回報為 *AWS CloudFormation Misconfiguration: Insecure EC2 AMI Storage*
- *Insecure Storage: Missing EFS Encryption* 現在會回報為 *AWS CloudFormation Misconfiguration: Insecure EFS Storage*
- *Insecure Storage: Missing Kinesis Stream Encryption* 現在會回報為 *AWS CloudFormation Misconfiguration: Insecure Kinesis Data Stream Storage*
- *Insecure Transport: Azure App Service* 現在會回報為 *Azure Ansible Misconfiguration: Insecure App Service Transport*
- *Kubernetes Bad Practices: API Server Publicly Accessible* 現在會回報為 *Azure ARM Misconfiguration: Improper AKS Network Access Control*
- *Privacy Violation: Exposed Default Value* 現在會回報為 *Azure ARM Misconfiguration: Hardcoded Secret*
- *Privilege Management: Overly Permissive Role* 現在會回報為 *Azure ARM Misconfiguration: Improper Custom Role Access Control Policy*

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 將對數千項弱點的檢查功能與指引使用者透過 SmartUpdate 即時取得下列可用更新的原則結合在一起：

弱點支援

Server-Side Request Forgery[5]

當攻**擊者可以影響應用程式伺服器建立的網路連線時，就會發生** Server-Side Request Forgery (SSRF)。網路連線來自應用程式伺服器的內部 IP，因而攻**擊者可以使用此連線略過網路控制措施**，並掃描或攻**擊原本未暴露的**內部資源。此發佈包括了一項檢查功能，可用於偵測接受使用者輸入的 Web 應用程式中是否有 SSRF 弱點。

Expression Language Injection[6]

CVE-2022-42889 已識別出在熱門的 Apache Commons Text 程式庫 1.5 到 1.9 版本中，存在一個嚴重的 Remote Code Execution 弱點。預設組態可能會允許進行不安全的 Script 評估及執行任意程式碼。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-2022-42889 弱點。由於這項檢查會傳送大量要求，所以被排除在標準原則之外。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。

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

Insecure Transport: Weak SSL Cipher

Transport Layer Security (TLS) 和 Secure Sockets Layer (SSL) 通訊協定提供機制，協助保護用戶端與 Web 伺服器之間所傳輸的資料的真實性、機密性和完整性。例如，使用低強度加密或長度不足的加密金鑰都可能會讓攻擊者突破保護機制，並竊取或修改敏感資訊。此版本包括一個識別碼 ID 為 11285 的新檢查功能，會將 Insufficient Transport Layer Protection - Insecure Cipher 弱點的嚴重性標記為「重大」。不安全的密碼加密套件存在多個已知弱點，並且已發生大小不一的攻擊。

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：

Insecure Transport: Weak SSL Cipher

此版本包括對 Insufficient Transport Layer Protection – Weak Cipher check (11716) 的改進。客戶應可看到這項檢查的嚴重性從「重大」降為「高」，因為針對這些弱式加密的攻擊非常精密，需要可觀的資源。我們已將這項檢查的嚴重性降低，並且引入新的檢查來識別「Insufficient Transport Layer Protection – Insecure Cipher」，同時將問題的嚴重性標記為「重大」。未來，建議使用的加密將不會納入沒有 Perfect Forward Secrecy (PFS) 的加密套件。

XML External Entity Injection[7]

由 ID 11337 所識別的檢查已修改為使用支援 Out-of-band Application Security Testing (OAST) 功能的有效酬載。改進這項檢查後，已減少誤報、提升效率，並提高其結果的準確性。

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。

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。

[7] 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
Software Security Research 經理
CyberRes Fortify
peter.blay@microfocus.com