Fortify 軟體安全性內容

2023 更新 2
2023 年 6 月 30 日

關於 OpenText Fortify Software Security Research

Fortify Software Security Research 團隊將尖端研究成果轉變為能夠為 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 31 種以上的語言支援 1,552 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，2023.2.0 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 31 種以上的語言偵測 1,329 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：

支援 Dart (支援的版本：2.19.6)[1]

Dart 軟體開發套件 (SDK) 由 Google 開發，提供強型別、以類別為基礎並且會執行記憶體回收的程式設計語言，用於建置桌面、行動和網頁應用程式。Dart 允許根據預期使用案例，將應用程式編譯到特定於架構的機器程式碼、可攜式模組或 JavaScript 之中，藉此提供多樣化的功能。使用 Dart 時，開發人員可以建立附有圖形使用者介面 (GUI) 的應用程式，使其成為建置多種軟體解決方案的靈活選擇。支援的類別包括：

- Access Control: Database
- Command Injection
- Denial of Service
- Denial of Service: Regular Expression
- Header Manipulation
- Insecure Transport
- Open Redirect
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Path Manipulation
- Privacy Violation
- Resource Injection
- Server-Side Request Forgery
- SQL Injection
- System Information Leak
- System Information Leak: Internal

初始支援 Flutter (支援的版本：3.7.11)[1]

Flutter 是 Google 建立的開放原始碼使用者介面 (UI) SDK，此 SDK 能夠充分發揮 Dart 程式設計語言的強大功能。它為開發人員提供一套全方位的工具、程式庫和套件，簡化了跨平台應用程式的建立流程。使用 Flutter 時，開發人員可以從單一程式碼庫建置行動、網頁和桌面應用程式，藉此簡化開發流程，並達到省時省力的效果。藉由利用 Flutter 的功能，開發人員可以建立具有視覺吸引力和高效能的應用程式，這些應用

[1] 需要 Fortify Static Code Analyzer 23.1.0。為獲得最佳結果，請使用 Fortify Static Code Analyzer 23.1.1。

程式可以跨多個平台無縫執行。對 Flutter 的支援包括追蹤使用者提供的輸入、偵測 Dart 程式設計語言支援的所有類別，以及以下專門用於 Flutter GUI 的類別：

- Privacy Violation: Shoulder Surfing
- System Information Leak: Internal

Android 13 (API 層級：33)

Android 平台是專為行動裝置設計的開放原始碼軟體堆疊。Android 的主要元件是 Java API Framework，用於向應用程式開發人員公開 Android 功能。此版本擴大了對使用 Java 或 Kotlin 編寫而成並利用 Android Java API Framework 之原生 Android 應用程式的弱點偵測。此版本針對 Android 應用程式引入了以下五種新的弱點類別：

- Privacy Violation: Android Insecure Indexing
- Privilege Management: Android Nearby Devices
- Privilege Management: Android Notifications
- Privilege Management: Android Read Aural Media
- Privilege Management: Android Read Visual Media

其他 Android 更新也涵蓋在內，以支援偵測以下命名空間中的現有弱點類別：

- android.app
- android.content
- android.net
- android.os
- android.util
- java.nio
- java.security
- java.security.interfaces

Java SE JDK (支援的版本：17)

Java Platform, Standard Edition (SE) Java Development Kit (JDK) 是一個軟體開發套件，包含用於開發 Java 應用程式與元件的工具和程式庫。此版本更新了對 Java SE JDK 15、16 和 17 中引入之新 API 的以下命名空間中現有弱點類別的支援：

- java.io
- java.lang
- java.lang.reflect
- java.net
- java.nio.channels
- java.util
- java.util.random
- java.util.stream

改進的掃描覆蓋範圍可能包括在以下類別下所確定的其他問題：

- Insecure Randomness
- Insecure Randomness: Hardcoded Seed
- Insecure Randomness: User-Controlled Seed
- Server-Side Request Forgery
- Setting Manipulation
- Unsafe Reflection

Kotlin 標準程式庫更新 (支援的版本：1.7.21)

Kotlin 是一種具有 Java 互通性的通用靜態型別語言。此版本包括對 Kotlin 版本 1.6 和 1.7 中引入之瞄準 Java 虛擬機器 (JVM) 的新標準程式庫 API 的更新支援。

Secret Scanning 更新

Secret Scanning 是一種在原始程式碼和組態檔案中自動搜尋 Secret 的技術。就此技術來說，「Secret」是指密碼、API 權杖、加密金鑰和應保密的類似構件。此版本包括對以下類別的 Secret Scanning 的更新支援：

- Credential Management: Hardcoded API Credentials
- Key Management: Hardcoded Encryption Key
- Password Management: Hardcoded Password

此外，以下類別現在支援 PowerShell 指令碼中的 Scret Sanning：

- Password Management: Hardcoded Password
- Privacy Violation

雲端基礎架構即程式碼 (IaC)

基礎架構即程式碼是透過程式碼 (而非各種手動程序) 來管理和佈建電腦資源的程序。擴展了受支援技術的涵蓋範圍，包括用於部署到 Amazon Web Services (AWS) 和 Google Cloud Platform (GCP) 的 Terraform 組態，以及 AWS CloudFormation 的組態。與上述服務組態設定相關的常見問題現在會回報給開發人員。

AWS 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 AWS 基礎架構的設定及管理。在此版本中，我們報告了有關 Terraform 組態的以下其他類別：

- AWS Terraform Misconfiguration: Aurora Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: CloudWatch Missing Customer-Managed Encryption Key

- AWS Terraform Misconfiguration: Database Migration Service Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: DocumentDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: ElastiCache Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Improper API Gateway Access Control
- AWS Terraform Misconfiguration: Improper EC2 Network Access Control
- AWS Terraform Misconfiguration: Improper ECR Access Control
- AWS Terraform Misconfiguration: Improper EKS Network Access Control
- AWS Terraform Misconfiguration: Improper ElastiCache Network Access Control
- AWS Terraform Misconfiguration: Improper Lambda Access Control
- AWS Terraform Misconfiguration: Improper MSK Network Access Control
- AWS Terraform Misconfiguration: Improper Neptune Access Control
- AWS Terraform Misconfiguration: Improper RDS Network Access Control
- AWS Terraform Misconfiguration: Improper S3 Access Control
- AWS Terraform Misconfiguration: Improper VPC Network Access Control
- AWS Terraform Misconfiguration: Insecure API Gateway Storage
- AWS Terraform Misconfiguration: Insecure API Gateway Transport
- AWS Terraform Misconfiguration: Insecure App Sync Storage
- AWS Terraform Misconfiguration: Insecure Athena Storage
- AWS Terraform Misconfiguration: Insecure CloudFront Transport
- AWS Terraform Misconfiguration: Insecure DynamoDB Storage
- AWS Terraform Misconfiguration: Insecure EC2 Storage
- AWS Terraform Misconfiguration: Insecure ECR Storage
- AWS Terraform Misconfiguration: Insecure ECS Transport
- AWS Terraform Misconfiguration: Insecure EKS Storage
- AWS Terraform Misconfiguration: Insecure ElastiCache Storage
- AWS Terraform Misconfiguration: Insecure Glue Storage
- AWS Terraform Misconfiguration: Insecure Kinesis Storage
- AWS Terraform Misconfiguration: Insecure MQ Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Transport
- AWS Terraform Misconfiguration: Insecure RDS Transport
- AWS Terraform Misconfiguration: Insecure S3 Storage
- AWS Terraform Misconfiguration: Insecure SageMaker Storage
- AWS Terraform Misconfiguration: Insufficient API Gateway Logging
- AWS Terraform Misconfiguration: Insufficient Aurora Backup
- AWS Terraform Misconfiguration: Insufficient CloudFront Logging
- AWS Terraform Misconfiguration: Insufficient CloudTrail Logging
- AWS Terraform Misconfiguration: Insufficient EC2 Logging
- AWS Terraform Misconfiguration: Insufficient ELB Logging
- AWS Terraform Misconfiguration: Insufficient ElastiCache Backup
- AWS Terraform Misconfiguration: Insufficient ElastiCache Logging
- AWS Terraform Misconfiguration: Insufficient Global Accelerator Logging
- AWS Terraform Misconfiguration: Insufficient GuardDuty Monitoring
- AWS Terraform Misconfiguration: Insufficient Lambda Logging
- AWS Terraform Misconfiguration: Insufficient OpenSearch Service Logging
- AWS Terraform Misconfiguration: Insufficient RDS Backup
- AWS Terraform Misconfiguration: Insufficient Redshift Logging
- AWS Terraform Misconfiguration: Insufficient S3 Backup
- AWS Terraform Misconfiguration: MemoryDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: MQ Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Neptune Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Reduced CloudFront Availability

- AWS Terraform Misconfiguration: Reduced ELB Availability
- AWS Terraform Misconfiguration: Reduced StackSets Availability
- AWS Terraform Misconfiguration: Weak Cognito Authentication
- AWS Terraform Misconfiguration: Weak IAM Password Policy

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 GCP 基礎架構的設定及管理。在此版本中，我們報告了有關 GCP Terraform 組態的以下弱點類別：

- GCP Terraform Misconfiguration: Insufficient Cloud Load Balancing Logging
- GCP Terraform Misconfiguration: Insufficient Cloud NAT Logging
- GCP Terraform Misconfiguration: Insufficient Media CDN Logging
- GCP Terraform Misconfiguration: Insufficient Operations Suite Logging

AWS CloudFormation 組態

CloudFormation 是 Amazon 提供的一項服務，用於自動佈建和設定 AWS 資源。CloudFormation 允許使用者使用 JSON 或 YAML 範本管理 AWS 資源。在此版本中，我們報告了有關 AWS CloudFormation 組態的以下弱點類別：

- AWS CloudFormation Misconfiguration: AmazonMQ Publicly Accessible
- AWS CloudFormation Misconfiguration: Backup Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: CloudTrail Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DataBrew Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Publicly Accessible
- AWS CloudFormation Misconfiguration: DocDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DocDBElastic Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DynamoDB Backup Disabled
- AWS CloudFormation Misconfiguration: EC2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ECR Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FinSpace Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FSx Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ImageBuilder Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Improper Athena Access Control
- AWS CloudFormation Misconfiguration: Improper CodeStar Access Control
- AWS CloudFormation Misconfiguration: Improper Cognito Access Control
- AWS CloudFormation Misconfiguration: Improper ECS Network Access Control
- AWS CloudFormation Misconfiguration: Improper EMR Access Control
- AWS CloudFormation Misconfiguration: Improper KMS Access Control
- AWS CloudFormation Misconfiguration: Improper Lambda Network Access Control
- AWS CloudFormation Misconfiguration: Improper Lightsail Access Control
- AWS CloudFormation Misconfiguration: Improper M2 Access Control

- AWS CloudFormation Misconfiguration: Improper QLDB Access Control
- AWS CloudFormation Misconfiguration: Improper RDS Access Control
- AWS CloudFormation Misconfiguration: Improper Redshift Access Control
- AWS CloudFormation Misconfiguration: Improper S3 Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Network Access Control
- AWS CloudFormation Misconfiguration: Improper Serverless Network Access Control
- AWS CloudFormation Misconfiguration: Improper Transfer Network Access Control
- AWS CloudFormation Misconfiguration: Insecure API Gateway Transport
- AWS CloudFormation Misconfiguration: Insecure CloudFront Transport
- AWS CloudFormation Misconfiguration: Insecure DAX Storage
- AWS CloudFormation Misconfiguration: Insecure ECR Supply Chain
- AWS CloudFormation Misconfiguration: Insecure EFS Storage
- AWS CloudFormation Misconfiguration: Insecure ELB Transport
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Storage
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Transport
- AWS CloudFormation Misconfiguration: Insecure WorkSpaces Storage
- AWS CloudFormation Misconfiguration: Insufficient API Gateway Logging
- AWS CloudFormation Misconfiguration: Insufficient AppSync Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Monitoring
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Config Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ECR Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ELB Logging
- AWS CloudFormation Misconfiguration: Insufficient ElasticLoadBalancing Logging
- AWS CloudFormation Misconfiguration: Insufficient Elasticsearch Logging
- AWS CloudFormation Misconfiguration: Insufficient GuardDuty Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Lambda Logging
- AWS CloudFormation Misconfiguration: Insufficient MQ Logging
- AWS CloudFormation Misconfiguration: Insufficient MSK Logging
- AWS CloudFormation Misconfiguration: Insufficient OpenSearch Service Logging
- AWS CloudFormation Misconfiguration: Insufficient RDS Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Route 53 Logging
- AWS CloudFormation Misconfiguration: Insufficient Serverless Logging
- AWS CloudFormation Misconfiguration: Insufficient Stack Monitoring
- AWS CloudFormation Misconfiguration: Kinesis Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Lambda Denial of Service
- AWS CloudFormation Misconfiguration: Location Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Logs Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: M2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: MemoryDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Neptune Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Privileged Batch Container
- AWS CloudFormation Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: RDS Publicly Accessible
- AWS CloudFormation Misconfiguration: Redshift Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Reduced EC2 Availability
- AWS CloudFormation Misconfiguration: Reduced ElastiCache Availability

- AWS CloudFormation Misconfiguration: Reduced Stack Availability
- AWS CloudFormation Misconfiguration: Rekognition Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: S3 Backup Disabled
- AWS CloudFormation Misconfiguration: SQS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: SageMaker Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Serverless Denial of Service
- AWS CloudFormation Misconfiguration: Timestream Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Weak API Gateway Authentication
- AWS CloudFormation Misconfiguration: Weak Certificate Manager Authentication
- AWS CloudFormation Misconfiguration: Weak IAM Authentication
- AWS CloudFormation Misconfiguration: Weak Lambda Authentication
- AWS CloudFormation Misconfiguration: Weak RDS Authentication

可自訂的密碼管理規則運算式更新

現在可以使用以下屬性指定 Salesforce Apex、Dart 和 PowerShell 指令碼的可自訂密碼管理規則運算式：

- com.fortify.sca.rules.password_regex.apex
- com.fortify.sca.rules.password_regex.dart
- com.fortify.sca.rules.password_regex.powershell

這些屬性可用於覆寫掃描 Salesforce Apex 原始程式碼、Dart 原始程式碼或 PowerShell 指令碼時用於識別密碼的預設規則運算式。

OWASP Mobile Application Security Verification Standard (MASVS) v2.0.0

OWASP MASVS v2.0.0 標準於 2023 年 4 月發布，是 OWASP Mobile Application Security (MAS) 專案的一部分。它為行動應用程式安全性要求提供了基準，旨在供行動軟體架構師、開發人員和測試人員使用。OWASP MASVS 2.0 旨在關注在行動裝置上執行的「用戶端」行動應用程式的應用程式安全性。因此，應將其與 OWASP ASVS 結合使用，以評估與遠端端點控制項相關的伺服器端應用程式安全性風險。為了支援我們的客戶開發安全的行動應用程式並評估行動應用程式的安全性控制涵蓋範圍和風險緩解，新增了 Fortify Taxonomy 與 OWASP MASVS v2.0.0 的關聯。

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「Access Control」類別

本版本中移除了 Salesforce Apex 的 *Access Control* 類別。缺少欄位層級安全性檢查現在會透過其他類別間接擷取，例如 *Access Control: Database* 和 *SOQL Injection*。

不再支援「Link Injection: Auto Dial」類別

Link Injection: Auto Dial 類別由於已經過時已被移除。引入此類別是為了解決 CVE-2017-2484 問題，以防止攻擊者利用 iOS 應用程式中未經淨化的使用者輸入來自動撥打電話號碼或 Facetime 通話。此漏洞已在 iOS 10.3 更新中修正，因此不再與目前的 iOS 應用程式相關。

棄用的標準對應

以下標準和最佳做法已標記為已過時，因此預設為不會顯示：

- CWE Top 25 2019
- CWE Top 25 2020
- DISA STIG 4.9
- DISA STIG 4.10
- OWASP Top 10 2004
- OWASP Top 10 2007
- OWASP Top 10 2010
- SANS Top 25 2009
- SANS Top 25 2010
- WASC 24 + 2

PHP 動態函數[2]

最新的 Fortify Static Code Analyzer 包括更新的 PHP 支援，支援針對未經淨化的外部輸入引用的動態函數回報 *Dynamic Code Evaluation: Code Injection* 問題。

Java 不安全類別

在 Java JDK 中，有一個隱藏類別，用於執行本質上不安全的操作，開發人員通常無法使用這些操作，需要使用反映功能才能執行個體化。現在，在 Java 專案中使用 `sun.misc.Unsafe` 類別時，掃描結果會將任何使用方法回報為 *Often Misused: sun.misc.Unsafe*。

[2] 需要 SCA 23.1 及更高版本

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: Unenforced Sharing Rules* – 已移除 Salesforce 觸發器、Visualforce 頁面和元件中的誤報
- *Command Injection* – 已移除 JavaScript 中標記規則運算式時的誤報
- *Cookie Security: Cookie not Sent Over SSL* – 在 Swift 中，已移除套用建議的補救措施時的誤報
- *Credential Management: Hardcoded API Credentials* – 已移除識別不記名權杖時的誤報
- *Dead Code: Expression is Always false* – 已移除 Java switch 陳述式中出現的誤報
- *Dockerfile Misconfiguration: Dependency Confusion* – 已移除有關 dockerfile 中「apt」和「apt-get」命令的誤報
- *Log Forging (debug)* – 在 Salesforce Apex 應用程式中，已移除列印 HTTP 要求標頭值時的誤報
- *Race Condition: Signal Handling* – 在 C/C++ 中，已移除叫用 `sigaction()` 時的誤報
- *String Termination Error* – 在 C++ 中，已移除觸發基元類型時的誤報
- *Unused Method* – 已移除 Java 程式碼中的誤報，其中方法由已實作的 Serializable 方法呼叫
- 已移除 JavaScript 中可能觸發布林值的資料流程誤報

類別變更

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

為了提高一致性，已重新命名以下類別：

- *Azure Terraform Misconfiguration: Improper CosmosDB CORS Policy* 現在會回報為 *Azure Terraform Misconfiguration: Improper Cosmos DB CORS Policy*
- *Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller* 現在會回報為 *Kubernetes Misconfiguration: Missing Service Account Admission Controller*
- *NoSQL Injection: CosmosDB* 現在會回報為 *NoSQL Injection: Cosmos DB*

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:

ZK Framework 是一個用於建立企業行動和網頁應用程式的開放原始碼 Java 程式庫，其中包含由 CVE-2022-36537 識別的安全性弱點。攻擊者可以利用此弱點擷取位於 Web 上下文中的檔案的內容。成功利用此弱點可使攻擊者獲取敏感資訊或瞄準原本可能無法存取的端點。此版本包含一項檢查功能，可用於偵測使用受影響 ZK Framework 版本的目標伺服器上是否有此弱點。

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：

Command Injection:

已新增由 ID 11722 和 11723 所識別的檢查，以使用支援 Out-of-band Application Security Testing (OAST) 功能的有效酬載[3]。這些檢查減少了誤報，提高了 WebInspect 掃描結果的準確性。

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。

OWASP MASVS v2.0.0

為了呼應新的關聯性，本版本也包含支援 OWASP MASVS v2.0.0 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。

[3] 由於 11723 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。

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。
與上述即時站點一致的 Fortify Taxonomy 站點的新雲端外版本，現在可供客戶從 Fortify 支援入口網站下載。

連絡 Fortify 技術支援

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