Fortify 軟體安全性內容

2023 更新 3
2023 年 9 月 29 日

關於 OpenText 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 33 種以上的語言支援 1,627 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，2023.3.0 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 1,403 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 Android 13 的支援 (支援的版本：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三種新的弱點類別：

- Intent Manipulation: Implicit Internal Intent
- Intent Manipulation: Implicit Pending Intent
- Intent Manipulation: Mutable Pending Intent

對 Android Jetpack (AndroidX) 的初始支援

Android Jetpack 是一組程式庫、工具和指南，可協助開發人員更輕鬆地建立 Android 應用程式。Jetpack 涵蓋 androidx.* 套件，並且從平台 API 中分離出來，有助於促進回溯相容性並允許更頻繁地更新。在此版本中，我們提供了這個軟體套件的初始涵蓋範圍。

Android Jetpack 的初始涵蓋範圍可支援偵測以下程式庫中的弱點：

- androidx.appsearch (version supported: 1.1.0-alpha03)
- androidx.compose.foundation (version supported: 1.5.1)
- androidx.compose.material (version supported: 1.5.1)
- androidx.compose.material3 (version supported: 1.1.2)
- androidx.compose.ui (version supported: 1.5.1)
- androidx.core (version supported: 1.12.0)
- androidx.credentials (version supported: 1.2.0-beta04)
- androidx.datastore (version supported: 1.0.0)
- androidx.security.crypto (version supported: 1.0.0)
- androidx.sqlite (version supported: 2.3.1)

範例類別涵蓋範圍的改進包括以下幾類：

- 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

MySQL Connector/Python 支援 (支援的版本：8.1.0)

MySQL Connector/Python 是一個軟體程式庫，可促進 Python 應用程式與 MySQL 資料庫之間的互動。它作為 Python 程式設計語言與 MySQL 資料庫管理系統之間的橋樑或連接器，讓開發人員能使用 Python 程式碼輕鬆連接、查詢及操作 MySQL 資料庫中的資料。

改進的類別涵蓋範圍包括如下：

- Access Control: Database
- Denial of Service
- Insecure Transport: Client Identity Verification Disabled
- Insecure Transport: Database
- Insecure Transport: Weak SSL Protocol
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Path Manipulation
- Server-Side Request Forgery
- SQL Injection

已改進對 Django 的支援 (支援的版本：3.2)

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。在此版本中，我們更新了現有的 Django 涵蓋範圍以支援最高版本 3.2。

改進的涵蓋範圍包括以下命名空間：*Django.contrib.auth.models*、*Django.db.models* 和 *Django.http.response*。此外，改進的弱點類別涵蓋範圍包括如下：

- Cookie Security: Overly Permissive SameSite Attribute
- Header Manipulation
- Password Management
- Password Management: Empty Password

- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- System Information Leak
- System Information Leak: External

對 Bicep 的初始支援 (支援的版本：0.21.1)[1]

Microsoft Bicep 是一種用於基礎架構即程式碼 (IaC) 解決方案的開放原始碼網域特定語言 (DSL)，由 Microsoft 開發，旨在簡化及流暢化 Azure 資源的部署。它會作為 Azure Resource Manager (ARM) 範本之上的抽象層，提供更直覺、更易讀取的方式來定義及管理 Azure 基礎架構。透過 Bicep，使用者可以編寫簡潔且人類可讀的程式碼，以用於描述 Azure 資源、組態和相依性。

弱點類別的初始涵蓋範圍包括如下：

- Azure ARM Misconfiguration: Automation Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Batch Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Cognitive Services Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Databricks Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Event Hubs Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Hardcoded Secret
- Azure ARM Misconfiguration: HTTPS Not Required
- Azure ARM Misconfiguration: Improper AKS Network Access Control
- Azure ARM Misconfiguration: Improper App Service Access Control
- Azure ARM Misconfiguration: Improper Blob Storage Access Control
- Azure ARM Misconfiguration: Improper Compute VM Access Control
- Azure ARM Misconfiguration: Improper Container Registry Network Access Control
- Azure ARM Misconfiguration: Improper CORS Policy
- Azure ARM Misconfiguration: Improper Custom Role Access Control Policy
- Azure ARM Misconfiguration: Improper DocumentDB Network Access Control
- Azure ARM Misconfiguration: Improper KeyVault Access Control Policy
- Azure ARM Misconfiguration: Improper Security Group Network Access Control
- Azure ARM Misconfiguration: Improper SQL Server Network Access Control
- Azure ARM Misconfiguration: Improper Storage Network Access Control
- Azure ARM Misconfiguration: Insecure Active Directory Domain Service Transport
- Azure ARM Misconfiguration: Insecure App Service Transport
- Azure ARM Misconfiguration: Insecure CDN Transport
- Azure ARM Misconfiguration: Insecure Database for MySQL Storage
- Azure ARM Misconfiguration: Insecure Database for PostgreSQL Storage
- Azure ARM Misconfiguration: Insecure DataBricks Storage
- Azure ARM Misconfiguration: Insecure EventHub Storage
- Azure ARM Misconfiguration: Insecure EventHub Transport
- Azure ARM Misconfiguration: Insecure IoT Hub Transport
- Azure ARM Misconfiguration: Insecure MySQL Server Transport
- Azure ARM Misconfiguration: Insecure PostgreSQL Server Transport

[1] 需要 Fortify Static Code Analyzer 23.2.0 版或更高版本。Bicep 的初始安全性內容隨 Fortify Static Code Analyzer 23.2.x 一起發行。

- Azure ARM Misconfiguration: Insecure Recovery Services Backup Storage
- Azure ARM Misconfiguration: Insecure Recovery Services Vaults Storage
- Azure ARM Misconfiguration: Insecure Redis Enterprise Transport
- Azure ARM Misconfiguration: Insecure Redis Transport
- Azure ARM Misconfiguration: Insecure Service Bus Storage
- Azure ARM Misconfiguration: Insecure Service Bus Transport
- Azure ARM Misconfiguration: Insecure Storage Account Storage
- Azure ARM Misconfiguration: Insecure Storage Account Transport
- Azure ARM Misconfiguration: Insufficient AKS Monitoring
- Azure ARM Misconfiguration: Insufficient Application Insights Logging
- Azure ARM Misconfiguration: Insufficient Application Insights Monitoring
- Azure ARM Misconfiguration: Insufficient Microsoft Defender Monitoring
- Azure ARM Misconfiguration: Insufficient SQL Server Logging
- Azure ARM Misconfiguration: Insufficient SQL Server Monitoring
- Azure ARM Misconfiguration: IoT Hub Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: NetApp Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Public Access Allowed
- Azure ARM Misconfiguration: Service Bus Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Storage Account Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Weak App Service Authentication
- Azure ARM Misconfiguration: Weak SignalR Authentication
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Privacy Violation
- Privacy Violation: Missing Secure Decorator

對 Solidity 的初始支援 (支援的版本： 0.8.x)[2]

Solidity 是一種物件導向的程式設計語言，用於在各種去中心化區塊鏈環境中開發智慧合約，尤其是在以太坊區塊鏈中。用 Solidity 編寫的智慧合約主要執行於以太坊虛擬機器 (EVM) 上，但也可以在其他相容的虛擬機器上執行。

弱點類別的初始涵蓋範圍包括如下：

- Authorization Bypass: tx.origin
- Code Correctness: Failing Assertion
- Code Correctness: Reentrancy
- Code Correctness: Typographical Error
- Dead Code
- Denial of Service: External Call
- Dynamic Code Evaluation: Delegatecall
- Integer Overflow
- Obsolete
- Often Misused: Block Values
- Poor Style: Confusing Naming

[2] 需要 Fortify Static Code Analyzer 23.2.0 版或更高版本。 Solidty 的初始安全性內容隨 Fortify Static Code Analyzer 23.2.x 一起發行。

- Poor Style: Variable Never Used
- Solidity Bad Practices: Default Function Visibility
- Solidity Bad Practices: Ether Balance Check
- Solidity Bad Practices: Hardcoded Gas Amount
- Solidity Bad Practices: Lack of Explicit Variable Visibility
- Solidity Bad Practices: Missing Constructor
- Solidity Misconfiguration: Compiler With Known Vulnerabilities
- Solidity Misconfiguration: Floating Pragma
- Unchecked Return Value
- Uninitialized Variable

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 Microsoft Azure 的 Terraform 組態以及 AWS Ansible 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。

Microsoft Azure 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 Microsoft Azure 基礎架構的設定及管理。改進的弱點類別涵蓋範圍包括 Terraform 組態的以下各類：

- Azure Terraform Misconfiguration: App Service Auto Upgrade Disabled
- Azure Terraform Misconfiguration: Improper AKS Access Control
- Azure Terraform Misconfiguration: Improper AKS Network Access Control
- Azure Terraform Misconfiguration: Improper App Service Access Control
- Azure Terraform Misconfiguration: Improper Cognitive Search Network Access Control
- Azure Terraform Misconfiguration: Improper Container Registry Access Control
- Azure Terraform Misconfiguration: Improper Functions Access Control
- Azure Terraform Misconfiguration: Improper MariaDB Network Access Control
- Azure Terraform Misconfiguration: Improper MySQL Network Access Control
- Azure Terraform Misconfiguration: Improper SQL Database Network Access Control
- Azure Terraform Misconfiguration: Improper Storage Account Access Control
- Azure Terraform Misconfiguration: Improper Virtual Network Access Control
- Azure Terraform Misconfiguration: Insecure Disk Storage
- Azure Terraform Misconfiguration: Insecure PostgreSQL Storage
- Azure Terraform Misconfiguration: Insufficient AKS Monitoring
- Azure Terraform Misconfiguration: Insufficient Application Gateway Monitoring
- Azure Terraform Misconfiguration: Insufficient Defender for Cloud Monitoring
- Azure Terraform Misconfiguration: Insufficient Front Door Monitoring
- Azure Terraform Misconfiguration: Insufficient MariaDB Backup
- Azure Terraform Misconfiguration: Insufficient Monitor Logging
- Azure Terraform Misconfiguration: Insufficient Network Watcher Logging
- Azure Terraform Misconfiguration: Insufficient PostgreSQL Monitoring
- Azure Terraform Misconfiguration: Insufficient SQL Database Monitoring
- Azure Terraform Misconfiguration: Redis Cache Auto Upgrade Disabled
- Azure Terraform Misconfiguration: Reduced Virtual Network Availability

- Azure Terraform Misconfiguration: Weak App Service Authentication
- Azure Terraform Misconfiguration: Weak Functions Authentication
- Azure Terraform Misconfiguration: Weak Linux Virtual Machines Authentication
- Azure Terraform Misconfiguration: Weak Service Fabric Authentication

Amazon Web Services (AWS) 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。改進的弱點類別涵蓋範圍包括 AWS Ansible 組態的以下各類：

- AWS Ansible Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS Ansible Misconfiguration: Improper API Gateway Network Access Control
- AWS Ansible Misconfiguration: Improper ECR Access Control
- AWS Ansible Misconfiguration: Improper ECS Network Access Control
- AWS Ansible Misconfiguration: Improper S3 Access Control
- AWS Ansible Misconfiguration: Improper Stack Access Control
- AWS Ansible Misconfiguration: Insecure API Gateway Transport
- AWS Ansible Misconfiguration: Insecure CloudFront Transport
- AWS Ansible Misconfiguration: Insecure CloudTrail Storage
- AWS Ansible Misconfiguration: Insecure CodeBuild Storage
- AWS Ansible Misconfiguration: Insecure RDS Transport
- AWS Ansible Misconfiguration: Insufficient API Gateway Logging
- AWS Ansible Misconfiguration: Insufficient CloudFront Logging
- AWS Ansible Misconfiguration: Insufficient Lambda Logging
- AWS Ansible Misconfiguration: Insufficient RDS Backup
- AWS Ansible Misconfiguration: Insufficient S3 Backup
- AWS Ansible Misconfiguration: Insufficient S3 Logging
- AWS Ansible Misconfiguration: Insufficient S3 Monitoring
- AWS Ansible Misconfiguration: Insufficient Stack Monitoring
- AWS Ansible Misconfiguration: Privileged Batch Container
- AWS Ansible Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Ansible Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS Ansible Misconfiguration: Reduced CloudFront Availability
- AWS Ansible Misconfiguration: Reduced EC2 Availability
- AWS Ansible Misconfiguration: Reduced ELB Availability
- AWS Ansible Misconfiguration: Weak IAM Password Policy

2023 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。2023 年 6 月發佈的 2023 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 Fortify Taxonomy 與 2023 CWE Top 25 之間的關聯性。

OWASP API Security Top 10 2023

Open Worldwide Application Security Project (OWASP) API Security Top 10 2023 提供了 2023 年影響 API 的前幾大安全性風險清單。其旨在提高對 API 安全性弱點的意識，並教育那些參與 API 開發和維護的人員，例如一般需要保護 Web API 的開發人員、設計人員、架構師、經理和/或組織。

OWASP API Security Top 10 側重於影響 Web API 的弱點，它並非單獨使用，而是要與其他標準和最佳實務做法結合使用，以全面捕獲所有相關的風險。例如：它應該與 OWASP Top 10 結合使用，以識別與輸入驗證 (例如 Injection) 相關的問題。為了向希望減輕 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 API Security Top 10 2023 之間的關聯性。

Center for Internet Security (CIS) 基準

Center for Internet Security (CIS) 基準是一系列由社群開發的安全組態建議，這些建議對應到 CIS Critical Security Controls。這些建議旨在確保雲端基礎架構的安全性，並證明其符合產業標準。CIS 基準會不斷更新，以適應所涵蓋的 25 多個廠商產品系列不斷演進的網路安全性狀態。支援的產品系列包括：

- Amazon Elastic Kubernetes Service (EKS) Benchmark v1.3.0
- Amazon Web Services Foundations Benchmark v2.0.0
- Azure Kubernetes Service (AKS) Benchmark v1.3.0
- Google Cloud Computing Platform Benchmark v2.0.0
- Google Kubernetes Engine (GKE) Benchmark v1.4.0
- Kubernetes Benchmark v1.7.1
- Microsoft Azure Foundations Benchmark v2.0.0

Smart Contract Weakness Classification (SWC)[3]

Smart Contract Weakness Classification (SWC) 是一種系統架構，用於分類及解釋智慧合約中的弱點。其提供一種標準化方法，來理解及解決這些在區塊鏈 (例如以太坊) 上執行之自動執行程式碼片段的弱點。值得注意的是，SWC 登錄的內容自 2020 年以來尚未全面更新，導致已知有不完整性、錯誤和重要遺漏之情況。為了向希望減輕智慧合約風險的客戶提供支援，已新增 Fortify Taxonomy 與目前版本 SWC 之間的關聯性。

[3] 需要 Fortify Static Code Analyzer 23.2.0 版或更高版本中的掃描功能。

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

正如 2022.4 版所觀察到的，我們將繼續支援 Fortify Static Code Analyzer 的最後四個主要版本。因此，這將是支援 20.x 之前的 Fortify Static Code Analyzer 版本的最後 Rulepack 版本。在下一個版本中，Fortify Static Code Analyzer 20.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 Fortify Static Code Analyzer 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。

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：

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* – 已移除與 ASP.NET 應用程式中虛擬欄位相關的誤報
- *Code Correctness: Double-Checked Locking* – 已移除 Java 應用程式中的誤報
- *Cross-Site Request Forgery* – 已移除 .NET 應用程式中使用 `AntiForgery.GetHtml()` 或 `Html.AntiForgeryToken()` 的 HTML 表單誤報
- *Cross-Site Scripting: Persistent* – 已移除 Django 應用程式中與 `cycle` 標籤相關的誤報
- *Double Free* – 已移除 C/C++ 應用程式使用來自 boost library 的 `throw_error()` 時的誤報
- *HTML5: Missing Content Security Policy* – 已移除 Java 應用程式中的誤報
- *JSON Injection* – 已移除 PHP 應用程式中的誤報
- *Mass Assignment: Insecure Binder Configuration* – 已移除 .NET 應用程式中與 Enum 類型相關的誤報
- *Often Misused: File System* – 已移除與 C++ 應用程式中 `GetFullPathNameW()` 和類似函數呼叫相關的誤報
- *Path Manipulation* – 已移除 Java 應用程式中使用 Amazon AWS SDK 時的誤報
- *Type Mismatch: Signed to Unsigned* – 已移除與 C/C++ 應用程式中布林值相關的誤報
- *Unreleased Resource* – 已移除 C++ 應用程式中使用 `CreateFileW()` 時的誤報

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 14 種類別：

移除的類別	新增的類別
AWS CloudFormation Misconfiguration: Insecure Elasticache Storage	AWS CloudFormation Misconfiguration: Insecure ElastiCache Storage
AWS CloudFormation Misconfiguration: Insecure Elasticache Transport	AWS CloudFormation Misconfiguration: Insecure ElastiCache Transport
AWS Terraform Misconfiguration: Elasticache Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
Azure Terraform Bad Practices: AKS Cluster Missing Host-Based Encryption	Azure Terraform Misconfiguration: AKS Cluster Missing Host-Based Encryption
Azure Terraform Bad Practices: Azure MySQL Server Missing Infrastructure Encryption	Azure Terraform Misconfiguration: MySQL Missing Infrastructure Encryption
Azure Terraform Bad Practices: Azure PostgreSQL Server Missing Infrastructure Encryption	Azure Terraform Misconfiguration: PostgreSQL Missing Infrastructure Encryption
Azure Terraform Bad Practices: Missing Azure Storage Infrastructure Encryption	Azure Terraform Misconfiguration: Storage Account Missing Infrastructure Encryption
Azure Terraform Bad Practices: Missing SQL Database Backup Encryption	Azure Terraform Misconfiguration: SQL Server Backup Missing Encryption
Azure Terraform Bad Practices: Scale Set Missing Host-Based Encryption	Azure Terraform Misconfiguration: Scale Set Missing Host-Based Encryption
Azure Terraform Bad Practices: VM Missing Host-Based Encryption	Azure Terraform Misconfiguration: VM Missing Host-Based Encryption
GCP Terraform Bad Practices: Overly Permissive Service Account	GCP Terraform Misconfiguration: Improper Compute Engine Access Control
GCP Terraform Misconfiguration: Weak Key Management	GCP Terraform Misconfiguration: Compute Engine Missing Customer-Managed Encryption Key
Kubernetes Bad Practices: Improper Admission Controller Access Control	Kubernetes Misconfiguration: Improper Admission Controller Access Control
Kubernetes Misconfiguration: Missing Service Account Admission Controller	Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller

Fortify 優先順序變更

為了提高與遺失客戶管理加密金鑰相關的弱點類別之間的一致性，以下 20 種類別的 Fortify 優先順序已變更為「低」：

- *Azure ARM Misconfiguration: Automation Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Batch Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Cognitive Services Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Databricks Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Event Hubs Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: IoT Hub Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: NetApp Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Service Bus Missing Customer-Managed Encryption Key*

- *Azure ARM Misconfiguration: Storage Account Missing Customer-Managed Encryption Key*
- *Azure Terraform Misconfiguration: AKS Cluster Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Azure Disk Snapshot Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Container Registry Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Cosmos DB Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Managed Disk Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Shared Image Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: SQL Database Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Storage Account Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Storage Encryption Scope Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: VM Storage Missing Customer-Managed Key*
- *GCP Terraform Misconfiguration: Compute Engine Missing Customer-Managed Encryption Key*

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

CVE-2023-25135 已識別出 vBulletin 5.6.0 版至 5.6.8 版中存在預先授權遠端程式碼執行 (RCE) 弱點。vBulletin 是一種用於建立動態線上社群和論壇的熱門軟體，它會不正確地清理使用者提供的輸入來進行未經驗證的還原序列化。此問題會讓攻擊者能在伺服器上執行任意程式碼、濫用應用程式邏輯或發動 Denial of Service (DoS) 攻擊。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。

Prototype Pollution：伺服器端

當攻擊者可以操縱物件的原型時，就會發生伺服器端 Prototype Pollution。這可能存在於以原型為基礎的語言 (例如 JavaScript) 中，這類語言允許在執行階段更改屬性和方法。此漏洞的嚴重性取決於應用程式中使用受污染物件的位置。攻擊包括 Denial of Service、變更應用程式組態，以及某些情況下的遠端程式碼執行。此版本包括了一項檢查功能，可用於偵測 Web 應用程式中是否有 Prototype Pollution。

合規報告

2023 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。6 月發佈的 2023 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。

OWASP API Security Top 10 2023

Open Worldwide Application Security Project (OWASP) API Security Top 10 2023 提供了 2023 年影響 API 的前幾大安全性風險清單。其旨在提高對 API 安全性弱點的意識，並教育那些參與 API 開發和維護的人員，例如一般需要保護 Web API 的開發人員、設計人員、架構師、經理和組織。OWASP API Security Top 10 側重於影響 Web API 的弱點，它並非單獨使用，而是要與其他標準和最佳實務做法結合使用，以全面捕獲所有相關的風險。例如：將 OWASP API Security Top 10 2023 與 OWASP Top 10 結合使用，以識別與輸入驗證 (例如 Injection) 相關的問題。此 SecureBase 更新包括新的合規報告範本，提供 OWASP API Security Top 10 2023 類別與 WebInspect 檢查之間的關聯性。

原則更新

2023 CWE Top 25

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 2023 CWE Top 25 相關的檢查而自訂的原則。

OWASP API Security Top 10 2023

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 OWASP API Security Top 10 2023 相關的檢查而自訂的原則。這些原則包含可用 WebInspect 檢查的子集，讓客戶能執行合規特定 WebInspect 掃描。

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。

LDAP Injection

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

SSL Certificate Hostname Discrepancy

SSL Certificate Hostname Discrepancy 檢查報告內容現在包括更詳細的資訊，可協助客戶針對此安全性問題應用正確的解決方案。

Aggressive Coverage by Check Inputs

對於某些 WebInspect 檢查，可以啟用 Aggressive Coverage，以指引 WebInspect 傳送一個瞄準更廣泛端點的更長攻擊清單。此版本包括對這些檢查的改進，讓客戶能透過變更 Check Inputs 來設定 Aggressive Coverage，而不是在掃描原則中新增不同的檢查。具有 Aggressive Coverage 功能的檢查包括以下各項：*Log4Shell*、*JNDI Reference Injection*、*Server-Side Request Forgery*、*OS Command Injection* 和 *Server-Side Prototype Pollution*。啟用 Aggressive Coverage 的檢查可提供更準確的掃描，但是，請務必考量要求數量和掃描時間可能會急劇增加。因此，Fortify 強烈建議您在單獨的原則中啟用 Aggressive Coverage 的情況下執行檢查，而不進行其他檢查。

Web Server Misconfiguration: Unprotected File

此版本包含一個輕微錯誤修正，以改進 Java 相關組態檔的偵測。

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。

2023 CWE Top 25

為了呼應新的關聯性，本版本也包含支援 2023 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。

OWASP API Security Top 10 2023

為了呼應新的關聯性，本版本也包含支援 OWASP API Security Top 10 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。

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。

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