Software Security Research 發佈公告

Fortify 軟體安全性內容

2021 更新 4

2021 年 12 月 17 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)、Fortify WebInspect 和 Fortify Application Defender) 增添動能的安全情報。現在，CyberRes Fortify 軟體安全性內容能夠跨 29 種語言支援 1,137 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，2021.4.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)，以及 Fortify Premium Content。

CyberRes Fortify Secure Coding Rulepack [SCA]

隨著此發佈，Fortify Secure Coding Rulepacks 能夠跨 29 種程式設計語言偵測 917 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 Core 和 ASP.NET 更新 (支援的版本： .NET Core 3.1)

已改進對各種 .NET Core 和 ASP.NET Core 命名空間的支援，包括以下各項：

- Microsoft.AspNetCore.Http
- Microsoft.AspNetCore.Mvc
- Microsoft.Extensions.Logging
- System
- System.IO
- System.Net
- System.Threading

此支援可以提高以下類別的涵蓋範圍：

- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak

Azure

Azure 是 Microsoft 的公有雲運算平台，提供包括運算、容器、物聯網、AI 和機器學習等一系列雲端服務。

在此版本中，我們將針對多項關鍵 Azure 服務提供初始支援：Functions、Identity 和 CosmosDB。除此之外，現在也支援以下特定 Azure 技術：

Azure Functions (支援的版本：Java 1.3.1、C# 3.x)

Functions 是 Microsoft Azure 的無伺服器運算解決方案。Azure Functions 提供持續更新的基礎架構來執行應用程式、建置 Web API、回應資料庫變更，以及管理訊息佇列。此更新包括對以下 C# 和 Java 觸發程序類型的初始支援：

- Blob Trigger
- CosmosDB Trigger
- Event Trigger
- Http Trigger (as class library)
- Http Trigger (as C# isolated process)
- Queue Trigger
- ServiceBus Trigger

Azure Functions 支援包括以下類別：

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Broad Domain
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial Of Service
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Overly Permissive CORS Policy
- Privacy Violation
- Resource Injection
- Setting Manipulation
- System Information Leak: External

Azure Identity (支援的版本：C# 1.5.0、Java 1.4.1)

Azure Identity 是 Microsoft 雲端型身分和存取管理服務，它會針對組織內的資源進行驗證和授權。此更新包括對以下命名空間的初始支援：

C#

- Azure.Identity (version 1.5.0)

Java

- com.azure.identity (version 1.4.1)

Azure Identity 支援包括以下類別：

- Password Management
- Password Management: Empty/Hardcoded/Null Password
- Password Management: Weak Cryptography
- Resource Injection

Azure CosmosDB (支援的版本：3.x)

Azure Cosmos DB 是一種全球分散式多模型資料庫服務。您可以透過 Azure Cosmos DB 使用 API 和程式設計模型來儲存和存取文件、鍵值、寬欄和圖形資料庫。此更新包括對以下 C# 命名空間的初始支援：

- Microsoft.Azure.Cosmos
- Microsoft.Azure.Cosmos.Scripts
- Microsoft.Azure.Cosmos.Table

Azure Cosmos DB 支援包括以下類別：

- Denial of Service
- HTML5: Overly Permissive CORS Policy
- Insecure Transport
- NoSQL Injection: CosmosDB
- Resource Injection
- Setting Manipulation
- SQL Injection

AWS

Amazon Web Services (AWS) 是一種公有雲運算平台，提供包括運算、儲存、網路、資料庫、物聯網和機器學習等一系列雲端服務。

在此版本中，我們將針對多項關鍵 AWS 服務提供初始支援：IAM、DynamoDB 和 RDS。此版本還新增了對 C# 的初始 Lambda 支援以及對 Java 的更新支援。除此之外，現在也支援以下特定 AWS 技術：

AWS Lambda 更新 (支援的版本：.NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x) [1]

Lambda 是一種運算服務，由 Amazon 提供並隸屬於 Amazon Web Services (AWS) 的一部分，它會直接執行程式碼而不需要佈建或管理伺服器。Lambda 服務會執行程式碼以回應事件，並自動管理程式碼所需的運算資源。此更新包括對 C# 的初始支援以及對 Java 的額外支援。此更新包括對以下 C# 和 Java 命名空間的支援：

C#

- Amazon.Lambda
- Amazon.Lambda.APIGatewayEvents
- Amazon.Lambda.Core

Java

- com.amazonaws.services.lambda.runtime
- com.amazonaws.services.lambda.runtime.events

此更新包括對以下事件類型的額外支援：

- API Gateway Events (C#, Java)

[1] 為了改進分析，請將 AWS SAM 或 CloudFormation YAML/JSON 範本納入翻譯範圍。

- DynamoDB (Java)
- S3 Events (Java)
- Scheduled Events (Java)

AWS Lambda 支援包括以下類別：

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- Log Forging
- Privacy Violation
- System Information Leak: External
- System Information Leak: Internal

AWS IAM (支援的版本：.NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x)

AWS Identity and Access Management (IAM) 是一種 Web 服務，用於控制對 AWS 資源的存取。IAM 可用於控制對 AWS 資源的驗證和授權使用。此更新包括對 C# 和 Java 的支援。此更新包括對以下 C# 和 Java 命名空間的支援：

C#

- Amazon.IdentityManagement.Model

Java

- com.amazonaws.services.identitymanagement.model
- software.amazon.awssdk.services.iam.model

除了識別敏感資訊之外，AWS IAM 支援還包括以下類別：

- Password Management
- Password Management: Empty/Hardcoded/Null Password
- Password Management: Weak Cryptography

AWS DynamoDB (支援的版本：.NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x)

AWS DynamoDB 是一種全代管 NoSQL 資料庫服務，支援鍵值和文件資料結構。DynamoDB 可用於儲存和擷取資料，並為任意數量的要求流量提供服務。此更新包括對 C# 的初始支援以及對 Java 的更新支援。支援包括以下命名空間：

C#

- Amazon.DynamoDBv2.Model
- Amazon.DynamoDBv2.DataModel
- Amazon.DynamoDBv2.DocumentModel

Java

- com.amazonaws.services.lambda.runtime.events.models.dynamodb
- software.amazon.awssdk.enhanced.dynamodb
- software.amazon.awssdk.enhanced.dynamodb.model

AWS DynamoDB 支援包括以下類別：

- Access Control: Database

- NoSQL Injection: DynamoDB
- SQL Injection: PartiQL

適用於 Aurora Serverless 的 AWS Relational Database Service (RDS) Data API (支援的版本：.NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x)

Amazon Aurora 是一種與 MySQL 和 PostgreSQL 相容的關聯式資料庫引擎，隸屬於代管 Amazon Relational Database Service (Amazon RDS) 的一部分。AWS RDS Data API 提供了 Web 服務介面，可讓應用程式能針對 Aurora Serverless 資料庫叢集存取並執行 SQL 陳述式。此更新包括對以下 C# 和 Java 命名空間的支援：

C#

- Amazon.RDSDataService.Model

Java

- software.amazon.awssdk.services.rdsdata.model (V2)

AWS RDS 支援包括以下類別：

- Access Control: Database
- Setting Manipulation
- SQL Injection

Secret Scanning

支援 Secret Scanning。Secret Scanning 是一種自動在文字檔中搜尋密碼的技術。在這種情況下，「密碼」是指密碼、API 權杖、加密金鑰，以及不得公開的類似構件。其主要目的是在原始程式碼和組態設定檔案中尋找意外硬編碼的密碼。現已透過新的 Regex 分析[2] 擴充對所有語言和其他檔案類型的支援。支援的類別包括：

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

Trojan Source

Trojan Source[3] 是 Nick Boucher 和 Ross Anderson 在他們的《Trojan Source: Invisible Vulnerabilities》報告中發佈的弱點類別。他們展示了 5 種不同的 Unicode 特殊字元使用方式，讓程式碼以一種方式呈現在開發人員眼前，但在執行時以不同的方式運作。Trojan Source 應被視為 Insider Threat 情境，即某個惡意個體可以故意插入 Unicode 字元。由於其中一個類別的精確性，所以我們將以下語言的偵測支援包含在 Core Rulepack 中：C、C++、C#、Go、Java、JavaScript、Python 和 Rust。支援的類別包括：

- Encoding Confusion: BiDi Control Characters

[2] 需要 Fortify Static Code Analyzer v21.2.0 或更高版本。
[3] 需要 Fortify Static Code Analyzer v21.2.0 或更高版本。

靜態/動態問題關聯[4]

支援匯出資料，以便在 Fortify Software Security Center (SSC) 中為 Java Spring 專案關聯靜態和動態掃描結果。支援的類別包括：

- Cross-Site Scripting: Content Sniffing
- Cross-Site Scripting: Inter Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- SQL Injection
- SQL Injection: Hibernate

已延伸 IBM Mainframe COBOL 支援 (支援的版本：6.3)

此更新包括偵測 IBM Mainframe COBOL 程式碼中的 Integer Overflow 弱點。

雲端基礎架構即程式碼

支援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。支援的技術包括 AWS、AWS CloudFormation、Azure ARM、Kubernetes K8S 和 Azure Kubernetes Service。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，包括：

- Access Control: Azure Blob Storage
- Access Control: Azure Container Registry
- Access Control: Azure Network Group
- Access Control: Azure SQL Database
- Access Control: Azure Storage
- Access Control: Cosmos DB
- Access Control: EC2
- Access Control: Kubernetes Admission Controller
- Access Control: Kubernetes Image Authorization Bypass
- Access Control: Overly Broad IAM Principal
- Access Control: Overly Permissive S3 Policy
- AKS Bad Practices: Missing Azure Monitor Integration
- Ansible Bad Practices: Missing CloudWatch Integration
- Ansible Bad Practices: Redshift Publicly Accessible
- Ansible Misconfiguration: Log Validation Disabled
- AWS CloudFormation Bad Practices: Missing CloudWatch Integration
- AWS CloudFormation Bad Practices: Redshift Publicly Accessible
- AWS CloudFormation Bad Practices: User-Bound IAM Policy
- AWS CloudFormation Misconfiguration: API Gateway Unauthenticated Access

---

[4] 需要 Fortify Static Code Analyzer v21.2.0 或更高版本。若要啟用關聯輸出，請在掃描時傳遞 `com.fortify.sca.rules.enable_wi_correlation` 屬性。如此一來，就可以使用命令列引數或透過修改 SCA 屬性檔案來完成。

- AWS CloudFormation Misconfiguration: Insecure Transport
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Logging
- AWS CloudFormation Misconfiguration: Insufficient DocumentDB Logging
- AWS CloudFormation Misconfiguration: Insufficient Neptune Logging
- AWS CloudFormation Misconfiguration: Insufficient RedShift Logging
- AWS CloudFormation Misconfiguration: Insufficient S3 Logging
- AWS CloudFormation Misconfiguration: Log Validation Disabled
- AWS CloudFormation Misconfiguration: root User Access Key
- AWS CloudFormation Misconfiguration: Unrestricted Lambda Principal
- Azure Monitor Misconfiguration: Insufficient Logging
- Azure Resource Manager Bad Practices: Cross-Tenant Replication
- Azure Resource Manager Bad Practices: Remote Debugging Enabled
- Azure Resource Manager Bad Practices: SSH Password Authentication
- Azure Resource Manager Misconfiguration: Insecure Transport
- Azure Resource Manager Misconfiguration: Overly Permissive CORS Policy
- Azure Resource Manager Misconfiguration: Security Alert Disabled
- Azure SQL Database Misconfiguration: Insufficient Logging
- Insecure SSL: Inadequate Certificate Verification
- Insecure Storage: Missing DocumentDB Encryption
- Insecure Storage: Missing EBS Encryption
- Insecure Storage: Missing Elasticache Encryption
- Insecure Storage: Missing Neptune Encryption
- Insecure Storage: Missing RDS Encryption
- Insecure Storage: Missing Redshift Encryption
- Insecure Storage: Missing S3 Encryption
- Insecure Storage: Missing SNS Topic Encryption
- Insecure Transport: Azure Storage
- Insecure Transport: Database
- Insecure Transport: Missing Elasticache Encryption
- Key Management: Excessive Expiration
- Kubernetes Bad Practices: API Server Publicly Accessible
- Kubernetes Bad Practices: Default Namespace
- Kubernetes Bad Practices: Host Write Access
- Kubernetes Bad Practices: Missing API Server Authorization
- Kubernetes Bad Practices: Missing Kubelet Authorization
- Kubernetes Bad Practices: Missing Node Authorization
- Kubernetes Bad Practices: Missing RBAC Authorization
- Kubernetes Bad Practices: NamespaceLifecycle Enforcement Disabled
- Kubernetes Bad Practices: readOnlyPort Enabled
- Kubernetes Bad Practices: Static Authentication Token
- Kubernetes Bad Practices: Unconfigured API Server Logging
- Kubernetes Misconfiguration: API Server Anonymous Access
- Kubernetes Misconfiguration: API Server Logging Disabled
- Kubernetes Misconfiguration: HTTP Basic Authentication
- Kubernetes Misconfiguration: Insecure Transport
- Kubernetes Misconfiguration: Kubelet Anonymous Access

- Kubernetes Misconfiguration: Missing Garbage Collection Threshold
- Kubernetes Misconfiguration: Missing Kubelet Client Certificate
- Kubernetes Misconfiguration: Overly Permissive Capabilities
- Kubernetes Misconfiguration: Privileged Container
- Kubernetes Misconfiguration: Server Identity Verification Disabled
- Kubernetes Misconfiguration: Unbound Controller Manager
- Kubernetes Misconfiguration: Unbound Scheduler
- Poor Logging Practice: Excessive Cloud Log Retention
- Poor Logging Practice: Insufficient Cloud Log Retention
- Poor Logging Practice: Insufficient Cloud Log Rotation
- Poor Logging Practice: Insufficient Cloud Log Size
- Privacy Violation: Exposed Default Value
- Privilege Management: Overly Broad Access Policy
- Privilege Management: Overly Permissive Role
- System Information Leak: Kubernetes Profiler

OWASP Top 10 2021

2021 年 Open Web Application Security Project (OWASP) Top 10 提供了一份強大的 Web 應用程式安全性意識文件，將重點放在讓社群瞭解最常見和最關鍵的 Web 應用程式安全性風險的後果。OWASP Top 10 呈現出對於最關鍵 Web 應用程式安全性漏洞的廣泛共識，並從資料收集和調查結果中取得共識。為了支援我們的客戶有效減輕 Web 應用程式風險，我們已新增 Micro Focus Fortify Taxonomy 與新發佈的 OWASP Top 10 2021 之間的關聯性。

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：

不再支援 18.x 之前的 Fortify Static Code Analyzer 版本：

如我們 2021.3 發佈公告中所述，這是支援 18.x 之前的 Fortify Static Code Analyzer 版本的最後 Rulepack 版本。在此版本中，Fortify Static Code Analyzer 18.x 之前的版本將不會載入 Rulepack。此時將會要求降級 Rulepack 或升級 SCA 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。

PHP 改進功能

已改進在 Key Management: Empty /Hardcoded/Null Encryption Key 類別中對於識別密碼和加密金鑰的支援。

Python 改進功能

已改進對 *subprocess* 模組的支援，從而改進對問題 (例如 Command Injection) 的偵測。

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：

- 在 Scala 專案中，當應用程式未使用 Play 時來自 Akka 執行者的問題。
- 在 JavaScript 中，只能取得對 URL 的部分控制時的 Cross-site Scripting 問題。
- 在 JSON 檔案中提及字串本地化時的 Password Management 問題
- 在 Java 和 .NET 專案中，來自 HTTP 方法的資料流問題。

CyberRes 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：

API Discovery

此版本包含一項用於 API Discovery 的檢查。當 WebInspect 在透過檢查輸入提供的使用者指定位置偵測到 swagger 規格 (spec) 中的 API 定義時，會標示 API Discovery 檢查。這些 spec 檔案可能不會在任何頁面中直接提及，因此不會在編目中偵測到。除了檢查 swagger 規格之外，在使用者指定的位置，系統也會透過檢查輸入，標示及測試掃描過程中發現的未明確指定定義。雖然這些發現不一定代表存在安全性弱點，卻會增加可能容易遭受攻擊的資源。

弱點支援

OGNL Expression Injection: 雙重評估

由 CVE-2021-26084 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 Atlassian 伺服器版本為 6.13.23 之前版本、6.14.0 版至 7.4.11 之前版本、7.5.0 版至 7.11.6 之前版本，以及 7.12.0 版至 7.12.5 之前版本。此版本包含一項檢查，可用來偵測受影響的 Atlassian 伺服器中是否存在此弱點。

Directory Traversal

Apache HTTP Server 已被發現容易遭受由 CVE-2021-41773 和 CVE-2021-42013 識別出的 Directory Traversal 攻擊。當 URL 對應到目錄 (由類似別名的指令所設定) 之外的檔案時，這些弱點可讓攻擊者能操縱這些 URL。攻擊者可能會復原伺服器上的檔案內容，進而導致敏感資料洩露、專有業務邏輯可能復原，以及針對某些組態設定的遠端程式碼執行。這些問題僅影響 Apache HTTP Server 2.4.49 版和 2.4.50 版。此版本包含一項檢查，用於偵測 Apache HTTP Server 中是否存在這些弱點。

Path Manipulation: Special Characters

由 CVE-2021-28164 識別出的 Path Manipulation 弱點會影響 Eclipse Jetty。若要求中的 URI 包含具有特殊字元的區段，則受影響版本中的預設合規模式會允許這類要求存取 WEB-INF 目錄中的受保護資源。如此就可能會公開有關 Web 應用程式實作的敏感資訊，並略過某些安全性限制。此版本包含一項檢查，用於偵測易受攻擊的 Jetty 執行個體。

Dynamic Code Evaluation: Unsafe XStream Deserialization

XStream 是一種常用的工具，用於在 Java 物件和 XML 之間轉換資料。解組時處理的資料流包含類型資訊，這些資訊可用於重新建立之前編寫的物件。攻擊者可以操縱處理後的輸入資料流，並取代或注入物件，從而導致執行從遠端伺服器載入的任意程式碼。此版本包含一項檢查，用於偵測目標網頁伺服器上是否存在最新的 Unsafe XStream Deserialization 弱點 CVE-2021-39149 弱點。

Path Manipulation: Special Characters

URL 路徑中不應允許使用諸如 0x09 之類的控制字元，這類字元必須由用戶端進行百分比編碼。若 Proxy 與後端伺服器之間對這些控制字元進行的剖析不一致，可能會帶來各種威脅。此版本包括一項檢查，用於偵測是否允許在 URL 路徑中插入一些常見的控制字元，以及是否會對後端網頁伺服器產生負面影響。

合規報告

OWASP Top 10 2021

2021 年 Open Web Application Security Project (OWASP) Top 10 提供了一份強大的 Web 應用程式安全性意識文件，將重點放在讓社群瞭解最常見和最關鍵的 Web 應用程式安全性風險的後果。OWASP Top 10 呈現出對於最關鍵 Web 應用程式安全性漏洞的廣泛共識，並從資料收集和調查結果中取得共識。此 SecureBase 更新包括新的合規報告範本，提供 OWASP Top 10 2021 類別與 WebInspect 檢查之間的關聯性。

原則更新

OWASP Top 10 2021

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 OWASP Top 10 2021 相關的檢查而自訂的原則。此原則包含可用 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：

SSL 檢查改進功能

已改進 SSL Cipher List 檢查，以反映以下組態設定不支援 Perfect Forward Secrecy：TLS_DH_RSA_WITH_AES_128_GCM_SHA256。

CyberRes 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 Top 10 2021

為了呼應新的關聯性，此版本也包含支援 OWASP Top 10 2021 的新報告套件，您可以從 Fortify 客戶支援入口網站的 Premium Content 下方進行下載。

CyberRes Fortify 分類法：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 CyberRes 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