Software Security Research 发行公告

Fortify 软件安全内容

2021 更新 4

2021 年 12 月 17 日

关于 CyberRes Fortify Software Security Research

Fortify Software Security Research 团队将尖端研究成果转换为助力 Fortify 产品组合（包括 Fortify Static Code Analyzer (SCA)、Fortify WebInspect 和 Fortify Application Defender）的安全情报。现在，CyberRes Fortify 软件安全内容支持 29 种语言的 1,137 个漏洞类别，且涵盖的单独 API 超过一百万个。
Fortify Software Security Research (SSR) 团队荣幸地宣布，我们即将推出对以下产品的更新：Fortify Secure Coding Rulepacks（2021.4.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）和 Fortify Premium Content。

CyberRes Fortify Secure Coding Rulepacks [SCA]

这次发行的 Fortify Secure Coding Rulepacks 可以检测 29 种编程语言的 917 个不同的漏洞类别，且涵盖的单独 API 超过一百万个。概括来说，此版本包括以下内容：

.NET Core 和 ASP.NET 更新（支持的版本：.NET Core 3.1）

改进了对多种 .NET Core 和 ASP.NET Core 命名空间的支持，包括以下各项：

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

该支持扩大了对以下类别的覆盖范围：

- 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 的公有云计算平台，提供包括计算、容器、物联网、人工智能和机器学习在内的各种云服务。

在此版本中，我们提供对多种主要 Azure 服务的初始支持：Functions、Identity 和 Cosmos DB。此外，现在还支持以下特定的 Azure 技术：

Azure Functions（支持的版本：Java 1.3.1、C# 3.x）

Functions 是 Microsoft Azure 的无服务器计算解决方案。Azure Functions 提供持续更新的基础设施来运行应用程序、构建 Web API、响应数据库更改以及管理消息队列。此更新包括对以下 C# 和 Java 触发器类型的初始支持：

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

Azure Functions 支持包括以下类别：

- 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（支持的版本：C# 1.5.0、Java 1.4.1）

Azure Identity 是 Microsoft 基于云的身份和访问管理服务。该服务提供对组织内资源的身份验证和授权。此更新包括对以下命名空间的初始支持：

C#

- Azure.Identity (version 1.5.0)

Java

- com.azure.identity (version 1.4.1)

Azure Identity 支持包括以下类别：

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

Azure Cosmos DB（支持的版本：3.x）

Azure Cosmos DB 是一种全球分布式多模型数据库服务。借助 Azure Cosmos DB，您可以使用 API 和编程模型来存储和访问文档、键值、宽列和图形数据库。此更新包括对以下 C# 命名空间的初始支持：

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

Azure Cosmos DB 支持包括以下类别：

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

AWS

Amazon Web Services (AWS) 是一个公有云计算平台，提供包括计算、存储、网络、数据库、物联网和机器学习在内的各种云服务。

在此版本中，我们提供对多个主要 AWS 服务的初始支持：IAM、DynamoDB 和 RDS。此版本还增加了对 C# 的初始 Lambda 支持以及对 Java 的更新支持。此外，现在还支持以下特定的 AWS 技术：

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

Lambda 是一种计算服务，由 Amazon 在 Amazon Web Services (AWS) 中提供，它可以运行代码而无需配置或管理服务器。Lambda 服务可通过运行代码来响应事件，并自动管理代码所需的计算资源。此更新包括对 C# 的初始支持以及对 Java 的附加支持。此更新包括对以下 C# 和 Java 命名空间的支持：

C#

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

Java

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

[1] 为了改进分析，请在转换时添加 AWS SAM 或 CloudFormation YAML/JSON 模板。

此更新包括对以下事件类型的附加支持：

- API Gateway Events（C#、Java）
- DynamoDB (Java)
- S3 Events (Java)
- Scheduled Events (Java)

AWS Lambda 支持包括以下类别：

- 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（支持的版本：.NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x）

AWS Identity 和 Access Management (IAM) 是控制 AWS 资源访问的 Web 服务。IAM 可用于控制在使用 AWS 资源时进行身份验证和授权。此更新包括对 C# 和 Java 的支持。此更新包括对以下 C# 和 Java 命名空间的支持：

C#

- Amazon.IdentityManagement.Model

Java

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

除了识别敏感信息之外，AWS IAM 支持还包括以下类别：

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

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

AWS DynamoDB 是完全托管的 NoSQL 数据库服务，支持键-值和文档数据结构。DynamoDB 可用于存储和检索数据，并为任意数量的请求流量提供服务。此更新包括对 C# 的初始支持以及对 Java 的更新支持。该支持包括以下命名空间：

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 支持包括以下类别：

- Access Control: Database
- NoSQL Injection: DynamoDB
- SQL Injection: PartiQL

AWS Relational Database Service (RDS) Data API for Aurora Serverless（支持的版本：.NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x）

Amazon Aurora 是与 MySQL 和 PostgreSQL 兼容的关系数据库引擎，该引擎属于托管 Amazon Relational Database Service (Amazon RDS) 的一部分。AWS RDS Data API 提供的 Web 服务接口支持应用程序针对 Aurora Serverless 数据库群集访问和执行 SQL 语句。此更新包括对以下 C# 和 Java 命名空间的支持：

C#

- Amazon.RDSDataService.Model

Java

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

AWS RDS 支持包括以下类别：

- Access Control: Database
- Setting Manipulation
- SQL Injection

Secret Scanning

支持 Secret Scanning。Secret Scanning 是一种能够在文本文件中自动搜索机密的技术。在此上下文中，“机密”指的是密码、API 令牌、加密密钥以及旨在保密的类似项目。其主要目的是在源代码和配置文件中查找意外硬编码的机密。通过新的正则表达式分析扩大了对所有语言和其他文件类型的支持[2]。支持的类别包括：

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

Trojan Source

Trojan Source[3] 是由 Nick Boucher 和 Ross Anderson 在他们的论文“Trojan Source: Invisible Vulnerabilities”（特洛伊之源：无形的漏洞）中发布的漏洞类别。他们展示了 5 种使用 Unicode 特殊字符使代码在开发人员肉眼看起来与实际执行时完全不同的方式。Trojan Source 应被视为是一种内部威胁，而恶意的个人可能会故意插入 Unicode 字符。由于其中一个类别的精确性，我们在内核规则包中加入了对以下语言的检测支持：C、C++、C#、Go、Java、JavaScript、Python 和 Rust。支持的类别包括：

- Encoding Confusion: BiDi Control Characters

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

Static/Dynamic Issue Correlation[4]

对于 Java Spring 项目，支持在 Fortify Software Security Center (SSC) 中导出数据以启用相关静态和动态扫描结果。支持的类别包括：

- 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

扩展的 IBM Mainframe COBOL 支持（支持的版本：6.3）

此更新包括对 IBM Mainframe COBOL 代码中的 Integer Overflow 漏洞的检测。

云基础设施即代码

支持云基础设施即代码 (IaC)。IaC 是指通过代码管理和配置计算资源的过程，而非多个手动过程。支持的技术包括 AWS、AWS CloudFormation、Azure ARM、Kubernetes K8S 和 Azure Kubernetes Service。与配置上述服务相关的常见问题现已报告给开发人员，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
- AWS CloudFormation Misconfiguration: Insecure Transport

[4] 需要使用 Fortify Static Code Analyzer v21.2.0 或更高版本。要启用相关输出，请在扫描时传递属性 'com.fortify.sca.rules.enable_wi_correlation'。此操作可通过命令行参数或通过修改 SCA 属性文件来完成。

- 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

开放式 Web 应用程序安全项目 (OWASP) Top 10 2021 提供了一份权威的 Web 应用程序安全意识文档，旨在向社区通报最常见、最严重的 Web 应用程序安全风险所带来的后果。OWASP Top 10 总结的十种最危险的 Web 应用程序安全漏洞得到了广泛认同，这种共识源自数据收集和调查结果。为了向希望降低 Web 应用程序风险的客户提供支持，我们增加了 Micro Focus Fortify Taxonomy 与新发布的 OWASP Top 10 2021 之间的关联。

杂项勘误表

在此版本中，我们已继续投入资源，以确保能够减少误报问题的数量，并提高客户审核问题的能力。此外，客户可能还会发现报告的与以下各项相关的问题发生了变化：

弃用版本低于 18.x 的 Fortify Static Code Analyzer：

正如 2021.3 发行公告中所述，这将是最后一次发行支持版本低于 Fortify Static Code Analyzer 18.x 的规则包。在此次发行中，版本低于 18.x 的 Fortify Static Code Analyzer 将不会加载规则包。这将需要对规则包进行降级或升级 SCA 版本。在未来的版本中，我们将继续支持 Fortify Static Code Analyzer 的最后四个主要版本。

PHP 改进

改进了对识别 Key Management: Empty /Hardcoded/Null Encryption Key 类别中密码和加密密钥的支持。

Python 改进

改进了对 *subprocess* 模块的支持，从而改进对 Command Injection 等问题的检测。

误报改进：

在此版本中，我们仍在继续致力于消除误报。除了其他改进之外，客户可能还会发现以下方面的误报也得以消除：

- 当应用程序未在使用 Play 时来自 Scala 项目中 Akka 参与者的问题。
- 当只能部分控制 URL 时 JavaScript 中出现的跨站点脚本攻击问题。
- 引用本地化后的字符串时 JSON 文件中出现的密码管理问题
- 来自 HTTP 方法的 Java 和 .NET 项目中出现的数据流问题。

CyberRes Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 不仅能对成千上万的漏洞进行检查，还可通过策略引导用户通过 SmartUpdate 立即获得以下更新：

API Discovery

此版本增加了对 API Discovery 的检查。当 WebInspect 在通过检查输入提供的用户指定位置处检测到 Swagger 规范中存在 API 定义时，将标记 API Discovery 检查。这些规范文件可能不会在任何页面中直接引用，因此不会在爬网中检测到。除了检查 Swagger 规范之外，还将在用户指定的位置处标记和测试在扫描期间发现的未通过检查输入明确指定的定义。虽然发现这些定义并不一定表明存在安全漏洞，但它们增加了可能容易受到攻击的资源。

漏洞支持

OGNL Expression Injection: Double Evaluation

标识为 CVE-2021-26084 的 OGNL Expression Injection 严重漏洞会影响 Atlassian Confluence Server 和 Data Center。此漏洞使未经身份验证的攻击者能够对存在漏洞的应用程序执行任意代码。受影响的 Atlassian 服务器版本为 6.13.23 之前的版本、从 6.14.0 到 7.4.11 之前的版本、从 7.5.0 到 7.11.6 之前的版本，以及从 7.12.0 到 7.12.5 之前的版本。此版本增加了一项检查，用于检测受影响的 Atlassian 服务器中是否存在此漏洞。

Directory Traversal

已发现 Apache HTTP Server 易受标识为 CVE-2021-41773 和 CVE-2021-42013 的 Directory Traversal 的攻击。这些漏洞使攻击者能够操纵 URL，而受操纵的 URL 会将 URL 映射到由类似别名的指令配置的目录之外的文件。攻击者可能会恢复服务器上各文件的内容，从而导致敏感数据泄露以及专有业务逻辑的潜在恢复，并且对于某些配置，还会导致远程代码执行。这些问题仅影响 Apache HTTP Server 2.4.49 和 2.4.50。此版本包含用于检测 Apache HTTP Server 中是否存在这些漏洞的检查功能。

Path Manipulation: Special Characters

标识为 CVE-2021-28164 的 Path Manipulation 漏洞会影响 Eclipse Jetty。受影响版本中的默认合规性模式允许带有 URI（包含具有特殊字符的段）的请求访问 WEB-INF 目录中受保护的资源。这可能会泄露有关 Web 应用程序实现的敏感信息，并绕过某些安全约束。此版本包含用于检测 Jetty 实例中是否存在此漏洞的检查功能。

Dynamic Code Evaluation: Unsafe XStream Deserialization

XStream 是在 Java 对象和 XML 之间转换数据的常用工具。解组时处理的流包含用于重新创建以前写入的对象的类型信息。攻击者可以操纵已处理的输入流并替换或注入对象，从而导致执行从远程服务器加载的任意代码。此版本增加了一项检查，用于检测目标 Web 服务器上是否存在不安全的最新 XStream 反序列化漏洞 CVE-2021-39149。

Path Manipulation: Special Characters

URL 路径中不应允许使用诸如 0x09 之类的控制字符，并且客户端必须对其进行百分比编码。代理服务器和后端服务器之间对这些控制字符的不一致解析可能会带来各种威胁。此版本增加了一项检查，用于检测是否允许在 URL 路径中插入一些常见的控制字符，以及这些字符是否会对后端 Web 服务器产生负面影响。

合规性报告

OWASP Top 10 2021

开放式 Web 应用程序安全项目 (OWASP) Top 10 2021 提供了一份权威的 Web 应用程序安全意识文档，旨在向社区通报最常见、最严重的 Web 应用程序安全风险所带来的后果。OWASP Top 10 总结的十种最危险的 Web 应用程序安全漏洞得到了广泛认同，这种共识源自数据收集和调查结果。此 SecureBase 更新包括一个新的合规性报告模板，可提供 OWASP Top 10 2021 类别与 WebInspect 检查之间的关联。

策略更新

OWASP Top 10 2021

在 WebInspect SecureBase 的支持策略列表中，添加了一项自定义策略以纳入与 OWASP Top 10 2021 相关的检查。该策略包含部分可用的 WebInspect 检查，支持客户运行特定于合规性的 WebInspect 检查。

杂项勘误表

在此版本中，我们已继续投入资源，以确保能够减少误报问题的数量，并提高客户审核问题的能力。此外，客户可能还会发现报告的与以下各项相关的问题发生了变化：

SSL 检查改进

改进了 SSL Cipher List 检查，以反映以下配置不支持完全正向保密：TLS_DH_RSA_WITH_AES_128_GCM_SHA256。

CyberRes Fortify Premium Content

此研究团队负责构建、扩展并维护我们的核心安全情报产品之外的各种资源。

OWASP Top 10 2021

除新关联之外，此版本还包含附带 OWASP Top 10 2021 支持的新报告包，您可从 Premium Content 下的 Fortify 客户支持门户下载该报告包。

CyberRes Fortify Taxonomy：软件安全错误

要访问 Fortify Taxonomy 站点以查看对新增类别支持的说明，请访问：https://vulncat.fortify.com。如果客户要从旧站点上查找最新支持的更新，可从 CyberRes Fortify 支持门户获取此更新内容。

联系 Fortify 技术支持

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

联系 SSR

Alexander M. Hoole
CyberRes Fortify Software Security Research 团队
高级经理
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
CyberRes Fortify Software Security Research 团队
经理
peter.blay@microfocus.com