Fortify 软件安全内容

2023 更新 2
2023 年 6 月 30 日

关于 OpenText 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) 和 Fortify WebInspect）的安全情报。现在，Fortify 软件安全内容支持超过 31 种语言的 1,552 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 Fortify Secure Coding Rulepacks（2023.2.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）和 Fortify Premium Content 的更新。

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

这次发行的 Fortify Secure Coding Rulepacks 可以检测超过 31 种语言的 1,329 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：

支持 Dart（支持的版本：2.19.6)[1]

由 Google 开发的 Dart 软件开发工具包 (SDK) 提供强类型、基于类和垃圾回收的编程语言，用于构建桌面、移动和 Web 应用程序。Dart 具有强大的通用性，允许根据预期用例将应用程序编译为特定于体系结构的机器代码、可移植模块或 JavaScript。凭借 Dart，开发人员可以创建带有图形用户界面 (GUI) 的应用程序，因而 Dart 是构建各种软件解决方案的灵活选择。支持的类别包括：

- 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

初步支持 Flutter（支持的版本：3.7.11)[1]

Flutter 是由 Google 开发的开源用户界面 (UI) SDK，能够充分发挥 Dart 编程语言的强大功能。它为开发人员提供了一套全面的工具、库和软件包，以方便创建跨平台应用程序。借助 Flutter，开发人员可以从单个代码库构建移动、Web 和桌面应用程序，从而简化开发流程并减少时间和精力。通过利用 Flutter 的功能，开发人员可以创建具有视觉吸引力和高性能的应用程序，这些应用程序能够跨多个平台无缝运行。对 Flutter

[1] 需要 Fortify Static Code Analyzer 23.1.0。为获得最佳效果，请使用 Fortify Static Code Analyzer 23.1.1。

的支持包括跟踪用户提供的输入，检测 Dart 编程语言所有支持的类别，以及以下专门针对 Flutter GUI 的类别：

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

Android 13（API 级别：33）

Android 平台是专为移动设备设计的开源软件堆栈。Android 的主要组件是 Java API 框架，它向应用程序开发人员开放 Android 功能。此版本扩展了使用 Java 或 Kotlin 编写并利用 Android Java API 框架的原生 Android 应用程序中的漏洞检测。此版本中为 Android 应用程序引入了五个新的缺陷类别：

- 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

另外，还包含其他 Android 更新，以支持检测以下命名空间中的现有缺陷类别：

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

Java SE JDK（支持的版本：17）

Java 平台标准版 (SE) Java 开发工具包 (JDK) 是一个软件开发包，其中包含用于开发 Java 应用程序和组件的工具和库。此版本包含对 Java SE JDK 15、16 和 17 中引入的新 API 的以下命名空间中的现有缺陷类别的更新支持：

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

改进的扫描覆盖范围可能包括以下类别中确定的其他问题：

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

Kotlin 标准库更新（支持的版本：1.7.21）

Kotlin 是一种通用的静态类型语言，具有 Java 互操作性。此版本包含对于针对 Java 虚拟机 (JVM) 的 Kotlin 版本 1.6 和 1.7 中引入的新标准库 API 的更新支持。

机密扫描更新

机密扫描是一种在源代码和配置文件中自动搜索机密的技术。在该上下文中，“机密”是指密码、API 令牌、加密密钥以及需要保密的类似项目。此版本包括对以下类别中机密扫描的更新支持：

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

此外，以下类别现在支持 PowerShell 脚本中的机密扫描：

- Password Management: Hardcoded Password
- Privacy Violation

云基础设施即代码 (IaC)

基础设施即代码是通过代码而非各种手动过程来管理和配置计算机资源的过程。受支持技术的扩展范围包括用于部署到 Amazon Web Services (AWS) 和 Google Cloud Platform (GCP) 的 Terraform 配置，以及用于 AWS CloudFormation 的配置。与上述服务配置相关的常见问题现已报告给开发人员。

AWS Terraform 配置

Terraform 是一种开源 IaC 工具，用于构建、更改云基础设施以及对其进行版本控制。它使用自己的声明性语言，称为 HashiCorp Configuration Language (HCL)。云基础设施被编码入配置文件以描述所需状态。Terraform 提供程序支持 AWS 基础设施的配置和管理。在此版本中，我们报告了 Terraform 配置中的以下附加类别：

- 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 配置

Terraform 是一种开源的基础设施即代码工具，用于构建、更改云基础设施以及对其进行版本控制。它使用自己的声明性语言，称为 HashiCorp Configuration Language (HCL)。云基础设施被编码入配置文件以描述所需状态。Terraform 提供程序支持配置并管理 GCP 基础设施。在此版本中，我们报告了 GCP Terraform 配置中的以下缺陷类别：

- 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 配置

CloudFormation 是 Amazon 提供的一项服务，用于自动设置和配置 AWS 资源。CloudFormation 允许用户使用 JSON 或 YAML 模板管理 AWS 资源。在此版本中，我们报告了 AWS CloudFormation 配置的以下缺陷类别：

- 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

可自定义密码管理正则表达式更新

现在可以使用以下属性指定 Salesforce Apex、Dart 和 PowerShell 脚本的可自定义密码管理正则表达式：

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

这些属性可用于覆盖在扫描 Salesforce Apex 源代码、Dart 源代码或 PowerShell 脚本时用于识别密码的默认正则表达式。

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

OWASP MASVS v2.0.0 标准于 2023 年 4 月发布，作为 OWASP Mobile Application Security (MAS) 项目的一部分。它提供了移动应用程序安全要求的基准，旨在供移动软件架构师、开发人员和测试人员使用。OWASP MASVS 2.0 旨在关注移动设备上运行的“客户端”移动应用程序的安全性。因此，它应与 OWASP ASVS 结合使用，以评估与远程端点控制相关的服务器端应用程序安全风险。为了支持我们的客户开发安全的移动应用程序并评估移动应用程序的安全控制覆盖范围和风险缓解，添加了 Fortify Taxonomy 与 OWASP MASVS v2.0.0 的关联。

杂项勘误表

在此版本中，我们已投入大量资源来确保能够减少误报问题的数量、重构以实现一致性并提高客户审核问题的能力。此外，客户可能还会发现与以下各项相关的已报告问题发生了变化：

弃用“Access Control”类别

Salesforce Apex 的 *Access Control* 类别已在此版本中移除。现在通过其他类别（例如 *Access Control: Database* 和 *SOQL Injection*）间接捕获缺乏字段级别安全检查的情况。

弃用“Link Injection: Auto Dial”类别

Link Injection: Auto Dial 类别因过时已被移除。引入该类别是为了解决 CVE-2017-2484 问题，其中攻击者可以利用 iOS 应用程序中未经净化的用户输入来自动拨打电话号码或 Facetime 通话。此漏洞已在 iOS 10.3 更新中修复，因此不再与当前的 iOS 应用程序相关。

已弃用的标准映射

以下标准和最佳实践已被标记为过时，因此默认情况下不会显示：

- 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 动态函数 [2]

最新的 Fortify Static Code Analyzer 包括更新的 PHP 支持，支持报告针对由未经净化的外部输入引用的动态函数的 *Dynamic Code Evaluation: Code Injection* 问题。

Java 不安全的类

Java JDK 中有一个隐藏类，用于执行本身不安全的操作，而需要反射来实例化的开发人员通常无法执行这些操作。现在，当在 Java 项目中使用 `sun.misc.Unsafe` 类时，扫描结果会将任何使用情况报告为 *Often Misused: sun.misc.Unsafe*。

[2] 需要 SCA 23.1 及更高版本

误报改进

此版本仍在继续努力改进，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得到了进一步消除：

- *Access Control: Unenforced Sharing Rules* – 消除了 Salesforce Trigger、Visualforce 页面和组件中的该误报
- *Command Injection* – 消除了在 JavaScript 中标记正则表达式时的该误报
- *Cookie Security: Cookie not Sent Over SSL* – 消除了应用建议的修正后 Swift 中的该误报
- *Credential Management: Hardcoded API Credentials* – 消除了识别持有者令牌时的该误报
- *Dead Code: Expression is Always false* – 消除了出现在 Java 开关语句中时的该误报
- *Dockerfile Misconfiguration: Dependency Confusion* – 消除了 dockerfile 中“apt”和“apt-get”命令的该误报
- *Log Forging (debug)*– 消除了打印 HTTP 请求标头值时 Salesforce Apex 应用程序中的该误报
- *Race Condition: Signal Handling* – 消除了调用 `sigaction()` 时 C/C++ 中的该误报
- *String Termination Error* – 消除了在 C++ 中触发基元类型时的该误报
- *Unused Method* – 消除了由已实现的可序列化方法调用方法的 Java 代码中的该误报
- JavaScript 中的数据流误报已消除，这些误报可能已经触发布尔值

类别更改

当缺陷类别名称发生更改时，将先前的扫描与新的扫描合并后的分析结果将导致增加/移除某些类别。

为了提高一致性，我们已对以下类别进行了重命名：

- *Azure Terraform Misconfiguration: Improper CosmosDB CORS Policy* 现在报告为 *Azure Terraform Misconfiguration: Improper Cosmos DB CORS Policy*
- *Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller* 现在报告为 *Kubernetes Misconfiguration: Missing Service Account Admission Controller*
- *NoSQL Injection: CosmosDB* 现在报告为 *NoSQL Injection: Cosmos DB*

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：

漏洞支持

Insecure Deployment: Unpatched Application:

ZK Framework 是用于创建企业移动和 Web 应用程序的开源 Java 库，包含标识为 CVE-2022-36537 的安全漏洞。攻击者可以利用此漏洞检索位于 Web 上下文中的文件的内容。成功利用该漏洞使攻击者能够获取敏感信息或瞄准原本可能无法访问的端点。此版本包括以下检查功能：在使用受影响的 ZK Framework 版本的目标服务器上检测是否存在此漏洞。

杂项勘误表

在此版本中，我们已投入大量资源来进一步减少误报数量，并提高客户审核问题的能力。此外，客户可能还会发现与以下各项相关的报告结果发生了变化：

Command Injection:

我们已添加标识为 ID 11722 和 11723 的检查功能以使用支持 Out-of-band Application Security Testing (OAST) 功能的有效负载[3]。这些检查功能可减少误报并提高 WebInspect 扫描结果的准确性。

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 MASVS v2.0.0

除新关联之外，此版本还包含附带 OWASP MASVS v2.0.0 支持的 Fortify Software Security Center 新报告包，您可从 Premium Content 下的 Fortify 客户支持门户下载该报告包。

[3] 因为 11723 检查会发送大量请求，所以其不包含在标准策略中。使用“所有检查”策略或自定义现有策略以包含此项检查，或者创建自定义策略来运行此项检查。

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。
与上述实时站点一致的新的 Fortify Taxonomy 站点云下版本现在可供客户从 Fortify 支持门户下载。

联系 Fortify 技术支持

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

联系 SSR

Alexander M. Hoole
Software Security Research 高级经理
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Software Security Research 经理
OpenText Fortify pblay@opentext.com
+1 (669) 309-1634