Fortify 软件安全内容

2024 更新 1
2024 年 3 月 29 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 OpenText™ Fortify Static Code Analyzer (SCA) 和 OpenText™ Fortify WebInspect）的安全情报。现在，Fortify 软件安全内容支持超过 33 种语言的 1,654 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（2024.1.0 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 33 种语言的 1,429 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：

改进了对 Angular 的支持（支持的版本：16.0.0）

Angular 是一个基于 TypeScript 的免费开源 Web 应用程序开发框架，专门用于创建 SPA（单页应用程序），且主要用于在前端动态高效地操作数据。将对 Angular 的支持从版本 11.2.4 扩展到 Angular 16.0.0（仅限初始支持）。Angular 结果已得到增强，以便客户可以获得有关以下类别的更准确结果，例如 *Cross-Site Request Forgery*、*Privacy Violation 和 System Information Leak*。扩展了对 JavaScript DOM 文档以及以下模块的覆盖范围：

- @angular/common/http
- @angular/core
- @angular/platform-browser

改进了对 PHP 的支持（支持的版本：8.2）

PHP 是一种广泛使用的通用脚本语言，最常用于 Web 开发。最新的 SSR 版本更新了对 PHP 的支持，最高可支持版本 8.2。具体来说，此版本包含了对 PHP 的以下附加基础扩展的初始支持：

- Sodium（支持的版本：8.3.1）

  PHP Sodium 扩展是 Libsodium 库的一种实现。Sodium 提供加密、解密、签名、密码哈希以及其他加密操作功能。客户可能会发现与加密和数字签名相关的其他问题，以及有关隐私侵权问题的更改。

- Zip（支持的版本：1.22.3）

  PHP Zip 扩展是 Libzip 库的一种实现。Zip 提供创建、修改和读取 zip 存档的功能，zip 存档是用于完成文件/数据分组和压缩的一种常见结构。该扩展的初始支持涵盖了特定于基本文件系统数据流的 ZipArchive 类，并扩展了 PHP 对以下类别的覆盖范围：

  - Key Management: Empty PBE Password
  - Path Manipulation: Zip Entry Overwrite

改进了对 Golang 的支持（支持的版本：1.21）[1]

Go（也称为 Golang）是在 Google 中创建的一种静态类型的编译型编程语言。它以简单、高效以及对并发的强大支持而知名，适合用于构建可扩展的 Web 服务、数据管道和分布式系统。Go 结合了编译型语言的性能优势以及解释型语言的编程简易性。其简洁的语法和强大的标准库使开发人员能够快速编写出准确的代码。扩展了对以下程序包的覆盖范围：

- context
- crypto/ecdh
- html/template
- net
- reflect
- Runtime
- time

云基础设施即代码 (IaC)[2]

扩展了对云基础设施即代码的支持。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。与上述服务配置相关的常见问题现已报告给开发人员。自 Fortify Static Code Analyzer 24.2 起，使用新技术报告 Azure ARM 和 AWS CloudFormation 配置问题。这会导致在合并使用 Fortify Static Code Analyzer 的先前版本生成的 FPR 时增加或消除一系列问题。使用 Fortify Static Code Analyzer 24.2 及更高版本时，需要使用规则包 2024.1 来防止出现重复的 IaC 问题。

Azure Resource Manager (ARM) 配置

ARM 是针对 Azure 的部署和管理服务。ARM 提供了一个管理层，可用于在 Azure 帐户中创建、更新和删除资源。

Amazon Web Services (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。利用这些模板，用户可以单个单元形式创建、删除和修改资源集合（称为堆栈）。在此版本中，我们报告了 AWS CloudFormation 配置中的以下其他缺陷类别：

- AWS CloudFormation Misconfiguration: Insecure SageMaker Transport
- AWS CloudFormation Misconfiguration: SageMaker Network Isolation Disabled
- AWS CloudFormation Misconfiguration: Weak SecretsManager Generated Password

[1] 为获取最准确的结果，请升级到 Fortify Static Code Analyzer 24.2 或更高版本。
[2] 需要 Fortify Static Code Analyzer 24.2 或更高版本。

改进了 Kotlin 支持（支持的版本：1.9.2)[3]

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以下 Kotlin 命名空间的 Kotlin 1.7.2、1.8 和 1.9 中引入的新标准库 API 的更新支持：*jvm.optional*、*math*、*io.path*、*coroutines.cancellation* 和 *kotlinx.serialization.json*。在现有类别中可能会检测到其他问题，包括：

- Denial of Service: Regular Expression
- Path Manipulation
- Privacy Violation
- System Information Leak

JavaScript/TypeScript Node.js 改进[4]

我们更新了 Node.js 规则，以便在使用 Fortify Static Code Analyzer 24.2 时能够利用类型解析优势。这些更改减少了误报，提高了命中率，并提升了 Node.js 应用程序中针对大多数类别的结果的准确性。更具体地说，客户会发现与以下 Node.js 模块相关的结果得到了改进：

- child_process
- dgram
- dns
- fs
- http
- https
- net
- querystring
- tls
- url
- util
- v8

还包括了对以下 NPM 程序包的初始部分支持：

- Bluebird
- child-process-promise

改进了 DISA STIG 5.3 支持

为了向联邦客户提供合规性方面的支持，我们更新了 Fortify Taxonomy 与美国国防信息系统局 (DISA) 应用安全与开发 STIG 版本 5.3 之间的关联以包括以下 45 个附加 STIG ID：APSC-DV-000010、APSC-DV-000210、APSC-DV-000230、APSC-DV-000240、APSC-DV-000330、APSC-DV-000380、APSC-DV-000390、APSC-DV-000400、APSC-DV-000410、APSC-DV-000430、APSC-DV-000450、APSC-DV-000580、APSC-DV-000590、APSC-DV-000710、APSC-DV-001120、APSC-DV-001130、APSC-DV-001280、APSC-DV-001290、APSC-DV-001300、APSC-DV-001310、APSC-DV-001320、APSC-DV-001330、APSC-DV-001410、APSC-DV-001520、APSC-DV-001530、APSC-DV-001540、APSC-DV-

[3] Kotlin 1.9 支持需要 Fortify Static Code Analyzer 24.2 或更高版本。

[4] 需要 Fortify Static Code Analyzer 24.2 或更高版本。

001610、APSC-DV-001760、APSC-DV-001770、APSC-DV-001780、APSC-DV-001790、APSC-DV-001795、APSC-DV-001820、APSC-DV-001970、APSC-DV-002290、APSC-DV-002310、APSC-DV-002320、APSC-DV-002410、APSC-DV-002530、APSC-DV-002890、APSC-DV-002950、APSC-DV-002960、APSC-DV-003100、APSC-DV-003310 和 APSC-DV-003320。

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：

减少误报和其他显著的检测改进

此版本仍在继续努力改进，消除误报。客户可以期待进一步消除误报，以及与以下方面相关的其他显著改进：

- *Access Control: Anonymous LDAP Bind* – 消除了 C/C++ 应用程序中的误报
- *Command Injection* – 在使用 Windows 版本的 C 运行时库函数的 C/C++ 应用程序中检测到新问题
- *Credential Management: Hardcoded API Credentials* – 消除了 YAML 文件中的误报
- *Dockerfile Misconfiguration: Dependency Confusion* – 消除了 Dockerfile 中与 npm 有关的误报
- *Dynamic Code Evaluation: Code Injection* – 在使用 Azure Cosmos DB API 的 ASP.NET 应用程序中检测到新问题
- *GCP Terraform Misconfiguration: Insecure Supply Chain* – 消除了 AWS Terraform 配置文件中的误报
- *Insecure SSL: Server Identity Verification Disabled* – 在使用 `Requests` 库的 Python 应用程序中检测到新问题
- *Mass Assignment: Insecure Binder Configuration* – 消除了 ASP.NET MVC 应用程序中的误报
- *Mass Assignment: Request Parameters Bound into Persisted Objects* – 消除了 Spring 应用程序中的误报
- *Password Management: Hardcoded Password* – 在 ODBC 连接字符串中检测到新问题
- *Poor Style: Identifier Contains Dollar Symbol ($)* – 消除了 Java 应用程序中的误报
- *Privacy Violation* – 在使用 Razor Pages 的 ASP.NET 应用程序中检测到新问题
- *Privacy Violation* – 在 Dart/Flutter 应用程序中检测到新问题
- *Privacy Violation* – 在使用 `csurf` 中间件以及 ExpressJS 库的 JavaScript 应用程序中检测到新问题
- *String Termination Error* – 在 C/C++ 应用程序中检测到新问题
- *System Information Leak: External* – 在使用 Razor Pages 的 ASP.NET 应用程序中检测到新问题
- *System Information Leak: External* – 在 C/C++ 应用程序中检测到新问题
- *Weak Encryption: Inadequate RSA Padding* – 消除了使用 OpenSSL 的 PHP 应用程序中的误报
- 消除了 Python Django 应用程序中的各种数据流误报

- 在 Java Spring 应用程序中检测到各种新的数据流问题
- 在 Java 扫描中，从 main() 入口点出现的各种数据流问题可能会显示为新问题和已消除的问题。这还会消除在 Kotlin 和 Scala 应用程序中发现的重复跟踪和错误跟踪。

类别名称更改

当缺陷类别名称发生更改时，将先前扫描的分析结果与新扫描相合并可能导致增加/移除某些类别。

为了提高一致性，我们已对以下四个类别进行了重命名：

2023 R4 类别名称	2024 R1 类别名称
Insecure Cross-Origin Opener Policy	HTML5: Insecure Cross-Origin Opener Policy
Insecure Transport: Client Identity Verification Disabled	Insecure SSL: Server Identity Verification Disabled
Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control	Kubernetes Terraform Misconfiguration: Improper DaemonSet Access Control
Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control	Kubernetes Terraform Misconfiguration: Improper StatefulSet Access Control

弃用“Header Checking Disabled”类别

此类别已被移除，以避免与其他类似名称的类别混淆。此类别中的先前规则现在报告为：

- ASP.NET Misconfiguration: Header Checking Disabled
- ASP.NET Misconfiguration: Unsafe Header Parsing

弃用某些“Dead Code”类别

以下“Dead Code”类别已从标准规则包中移除：

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: 未使用字段
- Dead Code: Unused Method
- Dead Code: Unused Parameter

对于希望继续看到检测到的这些漏洞的客户，可以从 Fortify 支持门户的单独规则包中下载这些规则。

OWASP Mobile Top 10 2023 重命名和弃用

继 2023 年 9 月发布“OWASP Top 10 Mobile Risks – Initial Release 2023”后，该项目于 2024 年 1 月完成并重命名为“OWASP Top 10 Mobile Risks – Final Release 2024”。因此，此版本包含“OWASP Mobile Top 10 Risks 2024”的附加映射和重命名映射。映射自身功能未发生更改。

在 Fortify 软件安全内容的下一个版本中，OWASP Mobile Top 10 2023 映射将被弃用，仅保留更新后的 OWASP Mobile Top 10 2024。

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 不仅能对成千上万的漏洞进行检查，还可通过策略引导客户使用 SmartUpdate 立即获得以下更新。

漏洞支持

Insecure Deployment: Unpatched Application (CVE-2024-23897)

Jenkins 是一个基于 Java 的自动化服务器，用于构建、测试和部署软件。Jenkins 命令行界面 (CLI) 是 Jenkins 的一项内置功能，可与 Jenkins 服务器进行交互，默认情况下处于启用状态。标识为 CVE-2024-23897 的严重文件读取漏洞允许在 Jenkins 中读取任意文件。此漏洞存在于用于解析提供给 CLI 的命令参数和选项的 args4j 库中。命令解析器具有一项功能，可以将参数中的 at 符号 (@) 字符（后跟文件路径）替换为指定文件的内容。受影响的 Jenkins 版本包括 2.441 及更早版本和 LTS 2.426.2 及更早版本。此版本包括用于检测目标服务器上是否存在 CVE-2024-23897 漏洞的检查功能。

Insecure Deployment: Unpatched Application (CVE-2023-22515)

Atlassian Confluence Data Center 和 Confluence 服务器为自托管解决方案，以为组织提供协作最佳实践而闻名。标识为 CVE-2023-22515 的严重访问控制漏洞允许恶意操作者创建未经授权的管理员帐户，从而授予他们对 Confluence 平台的不受限制的访问权限。即使攻击者缺少身份验证，他们也可以利用 CVE-2023-22515 建立未经授权的管理员帐户并访问 Confluence 实例。攻击者还可以操纵 Confluence 服务器设置，以表明设置过程尚未完成。Confluence Server 和 Confluence Data Center 受影响的版本为 8.0.0-8.0.4、8.1.0-8.1.4、8.2.0-8.2.3、8.3.0-8.3.2、8.4.0-8.4.2 和 8.5.0-8.5.1。此版本包括用于检测目标服务器上是否存在 CVE-2023-22515 漏洞的检查功能。

Insecure Deployment: Unpatched Application (CVE-2023-22518)

标识为 CVE-2023-22518 的严重不当授权漏洞会影响 Atlassian Confluence Data Center 和 Confluence 服务器。未经身份验证的攻击者会利用该漏洞重置 Confluence 并创建 Confluence 实例管理员帐户。凭借此帐户，攻击者可以执行 Confluence 实例管理员可执行的所有管理操作，从而导致机密性、完整性和可用性完全丧失。Confluence 服务器和 Confluence Data Center 受影响的版本为 7.19.16 之前的所有版本以及 8.3.4、8.4.4、8.5.3、8.6.1 版本。此版本包括用于检测目标服务器上是否存在 CVE-2023-22518 漏洞的检查功能。

OGNL Expression Injection: Double Evaluation (CVE-2023-22527)

标记为 CVE-2023-22527 的严重 OGNL Expression Injection 漏洞会影响 Atlassian Confluence 服务器和 Data Center。未经身份验证的攻击者可以利用此漏洞在易受攻击的应用程序上执行任意代码。Confluence Data Center 和 Confluence 服务器受影响的版本为 8.0.x、8.1.x、8.2.x、8.3.x、8.4.x 和 8.5.0-8.5.3。此版本包括用于检测受影响的 Atlassian 服务器中否存在此漏洞的检查功能。

合规性报告

Improved DISA STIG 5.3

为了向联邦客户提供合规性方面的支持，我们更新了 Fortify Taxonomy 与美国国防信息系统局 (DISA) 应用安全与开发 STIG 版本 5.3 之间的关联以包括以下 8 个附加 STIG ID：APSC-DV-000210、APSC-DV-000230、APSC-DV-000240、APSC-DV-000450、APSC-DV-001280、APSC-DV-001300、APSC-DV-002530 和 APSC-DV-003320。

策略更新

Improved DISA STIG 5.3

更新了 DISA STIG 5.3 策略以包括与 DISA STIG 5.3 相关的附加检查。

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。

XPath 注入

此版本包括对 *XPath Injection* 检查的改进，以减少误报并提高结果的准确性。

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 Mobile Top 10 2024

除重命名的 OWASP Mobile Top 10 Risks 2024 关联之外，此版本还包含附带 OWASP Mobile Top 10 2024 支持的 OpenText™ 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。

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。

联系 Fortify 客户支持

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