Software Security Research 发行公告

Fortify 软件安全内容

2022 更新 2

2022 年 6 月 24 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) 和 Fortify WebInspect）的安全情报。现在，Fortify 软件安全内容支持 30 种语言的 1,220 个漏洞类别，且涵盖的单独 API 超过一百万个。

Fortify 软件安全研究 (SSR) 团队荣幸地宣布，我们即将推出 Fortify Secure Coding Rulepack（2022.2.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）和 Fortify Premium Content 的更新。

Fortify Secure Coding Rulepack [SCA]

这次发行的 Fortify Secure Coding Rulepack 可以检测 30 种编程语言的 1,000 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 改进（支持的版本：6.0）

.NET 是一个通用编程平台，使程序员能够使用一组标准化的 API 采用 C# 和 VB.NET 等语言编写代码。此版本将我们的覆盖范围扩大到最新版本的 .NET 以改进数据流，同时将 API 覆盖范围扩展到以下类别：

- Access Control: Database
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- SQL Injection
- System Information Leak: External
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Encryption: Insecure Mode of Operation

ASP.NET Core 改进（支持的版本：6.0）

ASP.NET Core 是用于 .NET 的 Web 旗舰框架。该框架具备创建多种类型的应用程序的功能，包括 MVC Web 应用程序和 Web API。此版本将我们的覆盖范围扩大到最新版本的 ASP.NET Core，包含极少的 API，同时将支持的类别扩展为包括：

- .NET Attribute Misuse: Authorization Bypass
- ASP.NET Bad Practices: Compression Over Encrypted WebSocket Connection
- ASP.NET Middleware Out of Order: Default Cookie Configuration
- ASP.NET Middleware Out of Order: Insecure Transport
- ASP.NET Middleware Out of Order: Insufficient Logging
- ASP.NET Misconfiguration: Insecure Transport
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute

Weak Cryptographic Implementation

Psychic Signatures (CVE-2022-21449) 是椭圆曲线数字签名算法 (ECDSA) 的 Java 实现中的一个缺陷。攻击者可利用此缺陷强制应用程序接受全零数字签名为有效签名。易受攻击的 Java 版本包括：15、16、17 和 18。如果使用易受攻击的 Java 版本，攻击者可以伪造某些类型的 SSL 证书、签名的 JSON Web 令牌，甚至是 WebAuthn 身份验证消息。此版本增加了对在 Java 中报告 *Weak Cryptographic Implementation* 的支持。

Jakarta EE 支持（支持的版本：9.0.0）

Jakarta EE 以开源框架的形式提供一套全面的与供应商无关的开放规范，用于开发云原生 Java 应用程序。该框架以前称为 Java EE（或 J2EE），是最知名的服务器端 Java 框架之一。此版本增加了对现有 Java EE 覆盖范围的改进，涉及 52 个缺陷类别。

密码扫描改进

密码扫描是一种在源代码和配置文件中搜索和检测密码的技术。有时，包含密码或 API 令牌的配置文件可能会意外泄露到源代码存储库。此版本包括对常见密码哈希格式的支持。覆盖范围包括识别常见密码哈希格式和产品配置文件中的密码，包括以下内容：OpenVPN、Windows 远程桌面、netrc、IntelliJ IDEA、DBeaver、FileZilla、Heroku 和 DigitalOcean doctl。
增强了对以下类别的覆盖范围：

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Password Management: Hardcoded Password
- Password Management: Password in Configuration File
- Password Management: Weak Cryptography

Express JS 改进（支持的版本：4.x）[1]

Express 是一个使用 Node.js 构建 Web 应用程序的框架。该框架提供用于路由、错误处理、模板化、中间件管理和 HTTP 相关实用程序的功能。
在此版本中，我们改进了对 Express 4.x 的以下类别的支持：

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Insecure Transport
- Path Manipulation
- Privacy Violation
- Process Control
- Setting Manipulation
- System Information Leak: External

JavaScript Handlebars（支持的版本：4.7.7）

Handlebars 是一个 JavaScript 库，旨在制作可重用的 Web 模板。这些模板由 HTML、文本和表达式组合而成。表达式直接嵌入到 HTML 代码中，并充当要由代码插入的内容的占位符，从而使文档易于重用。

[1] 需要 SCA 版本 22.1.1

在此版本中，我们增加了对 Handlebars 4.7.7 的支持，改进了数据流覆盖范围，并将 API 覆盖范围扩展到以下类别：

- Cross-Site Scripting: Handlebars Helper
- Handlebars Misconfiguration: Escaping Disabled
- Handlebars Misconfiguration: Prototypes Allowed
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak
- Template Injection

JavaScript Mustache（支持的版本：4.2.0）

Mustache 是一个开源的无逻辑模板系统，它提供模板和视图，作为创建动态模板的基础。模板包含演示格式和代码，而视图包含模板中要包含的数据。
在此版本中，我们添加了对 Mustache 4.2.0 的支持，用以识别 *Template Injection* 缺陷。

GraphQL.js（支持的版本：16.5.0）

GraphQL.js 是 GraphQL 的 JavaScript 参考实现，广泛用于 JavaScript 应用程序。此版本添加了初始 GraphQL 服务器支持，以检测 GraphQL API 中的以下缺陷类别：

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled
- Privacy Violation
- System Information Leak: External

Graphene-Python（支持的版本：3.0.0）

Python-Graphene 是用于 Python 应用程序的常用 GraphQL 服务器框架。此版本改进了 2022.1.0 版的 GraphQL 服务器支持，以检测 GraphQL API 中的以下缺陷类别：

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Privacy Violation
- System Information Leak: External

云基础设施即代码

基础设施即代码 (IaC) 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。此版本扩展了对 IaC 的支持。支持的技术包括用于部署到 Azure 和 AWS 的 Ansible 配置，以及用于部署到 Azure 和 GCP 的 Terraform 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。

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 ***Microsoft Azure*** 基础设施的配置和管理。在此版本中，我们报告了 Microsoft Azure 服务的 Terraform 配置中的以下缺陷类别：

- Azure Terraform Misconfiguration: Insecure App Service Transport
- Azure Terraform Misconfiguration: Insecure CDN Endpoint Transport
- Azure Terraform Misconfiguration: Insecure Function App Transport
- Azure Terraform Misconfiguration: Insecure Logic App Transport
- Azure Terraform Misconfiguration: Insecure MariaDB Transport
- Azure Terraform Misconfiguration: Insecure MySQL Transport
- Azure Terraform Misconfiguration: Insecure Network Monitor Transport
- Azure Terraform Misconfiguration: Insecure PostgresSQL Transport
- Azure Terraform Misconfiguration: Insecure Redis Cache Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Redis Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Transport
- Azure Terraform Misconfiguration: Insecure Storage Account Transport

Terraform 提供程序支持 ***Google Cloud Platform (GCP)*** 基础设施的配置和管理。在此版本中，我们报告了 Google Cloud Platform 的 Terraform 配置中的以下缺陷类别：

- GCP Terraform Bad Practice: Overly Permissive Service Account
- GCP Terraform Misconfiguration: BigQuery Dataset Publicly Accessible
- GCP Terraform Misconfiguration: Cloud DNS DNSSEC Disabled
- GCP Terraform Misconfiguration: Cloud KMS CryptoKey Publicly Accessible
- GCP Terraform Misconfiguration: Cloud SQL Backup Disabled
- GCP Terraform Misconfiguration: Cloud Storage Bucket Publicly Accessible
- GCP Terraform Misconfiguration: Compute Engine Access Control
- GCP Terraform Misconfiguration: Compute Engine Default Service Account
- GCP Terraform Misconfiguration: Compute Engine Project-Wide SSH
- GCP Terraform Misconfiguration: Google Project Network Access Control
- GCP Terraform Misconfiguration: Insecure Cloud SQL Transport
- GCP Terraform Misconfiguration: Insecure Load Balancer Transport
- GCP Terraform Misconfiguration: Insufficient Cloud Storage Bucket Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Monitoring
- GCP Terraform Misconfiguration: Insufficient VPC Flow Logging
- GCP Terraform Misconfiguration: GKE Cluster Administrative Interface Access Control
- GCP Terraform Misconfiguration: GKE Cluster Certificate-Based Authentication
- GCP Terraform Misconfiguration: GKE Cluster Legacy Authorization
- GCP Terraform Misconfiguration: GKE Cluster HTTP Basic Authentication
- GCP Terraform Misconfiguration: GKE Container-Optimized OS Not In Use
- GCP Terraform Misconfiguration: GKE Node Auto-Upgrade Disabled

- GCP Terraform Misconfiguration: Weak Cryptographic Cloud DNS Signature
- GCP Terraform Misconfiguration: Weak GKE Cluster Network Management
- GCP Terraform Misconfiguration: Weak Key Management

Ansible 配置：
Ansible 是一种开源自动化工具，可提供对各种环境的配置管理、应用程序部署、云配置和节点编排。

Ansible 包含支持配置和管理 ***Amazon Web Services (AWS)*** 的模块。在此版本中，我们报告了 AWS Ansible 配置的以下缺陷类别：

- AWS Ansible Misconfiguration: Amazon RDS Publicly Accessible
- AWS Ansible Misconfiguration: Insecure CloudFront Distribution Transport
- AWS Ansible Misconfiguration: Insufficient CloudTrail Logging

Ansible 还包括支持配置和管理 ***Microsoft Azure 云计算服务***的模块。在此版本中，我们报告了 Microsoft Azure 的 Ansible 配置中的以下缺陷类别：

- Azure Ansible Misconfiguration: Overly Permissive Azure SQL Database Firewall

杂项勘误表

在此版本中，我们继续投入资源，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，客户可能还会发现与以下各项相关的已报告问题发生了变化：

Log4j（支持的版本：2.17）

对 Log4j 的支持现在包括检测新类别 *Denial of Service: Stack Exhaustion*。

Oslo.config（支持的版本：8.8.0）

对 Python 的 oslo.config 的初始支持包括检测新类别 *Privacy Violation: Unobfuscated Logging*。

Objective-C 错误修复和性能改进

客户在使用 2022R1 规则包扫描包含 Objective-C 文件的项目时，可能会遇到以下问题：

- 在扫描阶段，SCA 输出或日志文件中可能会出现“[error] Unexpected exception during dataflow analysis...”形式的错误消息
- 执行数据流分析时的扫描时间异常长，可能会导致数据流丢失问题

我们向受影响的客户提供了 Objective-C 修补程序规则包以解决这些问题。此 R2 官方版本中包含相同的修补程序。使用修补程序规则包的客户应在更新到 R2 版本规则包后删除修补程序规则包。

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：

- *SQL Injection: iBatis Data Map* - 防止了遇到文本“$”字符时出现该误报
- *Password Management: Password in Configuration File* - 防止了值为变量占位符时出现该误报
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property* - 防止了使用 [BindRequired] 属性时在 C# ASP.NET 应用程序中出现该误报
- *Often Misused: Authentication* - 减少了在 Java 应用程序中出现该误报
- *XSS: Content Sniffing* - 减少了在 Java Spring 应用程序中出现该误报
- *Privacy Violation* - 减少了在 .NET 应用程序中出现该误报
- *SOQL Injection* 和 *SOSL Injection* - 语义分析器发现的问题现在以低 Fortify 优先级报告

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

OGNL Expression Injection: Double Evaluation

标记为 CVE-2022-26134 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。受影响的 Confluence 服务器和 Data Center 版本为 1.3.0 至 7.4.16、7.13.0 至 7.13.6、7.14.0 至 7.14.2、7.15.0 至 7.15.1、7.16.0 至 7.16.3、7.17.0 至 7.17.3 以及 7.18.0。此版本包括用于检测受影响的 Confluence 和 Data Center 服务器中是否存在此漏洞的检查功能。

Dynamic Code Evaluation: Code Injection

Pivotal 开发的 Spring Framework 容易受到标记为 CVE-2022-22965 的 Remote Code Execution (RCE) 漏洞的攻击。远程攻击者可提供特别构造的请求参数，从而导致执行任意代码。此版本包括用于检测使用受影响的 Spring Framework 版本的 Web 应用程序中是否存在此漏洞的检查功能。

Insecure Deployment: OpenSSL

OpenSSL 是一种广泛用于支持 SSL/TLS 连接的常用加密库，其容易受到标记为 CVE-2022-0778 的 Denial of Service (DoS) 漏洞的攻击。通过制作具有无效显式椭圆曲线参数的证书，可以在受影响的系统上触发无限循环 DoS。此版本包括用于检测目标 Web 服务器上是否存在 CVE-2022-0778 漏洞的检查功能。由于此项检查有可能导致在受影响的系统上生成 DoS 条件，从而导致该系统无法提供服务，因此此项检查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。

杂项勘误表

在此版本中，我们继续投入资源，以减少误报问题的数量，并提高客户审核问题的能力。此外，客户可能还会发现与以下各项相关的报告结果发生了变化：

Password Management: Weak Password Policy

此版本包含对密码策略检查的细微改进，当输入类型为文本框时，可以更准确地识别密码/用户名字段。

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。

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

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