Software Security Research 发行公告

Fortify 软件安全内容

2022 更新 1

2022 年 3 月 25 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 1,166 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（2022.1.0 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 946 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：

Log4j 更新（支持的版本：2.17）

Log4j 是一款受欢迎的 Java 日志框架，但最近几个月该框架受到审查，因为在该框架内发现一些备受关注的漏洞。此版本包括改进的支持，可准确识别源代码的哪些部分易受 Log4Shell 漏洞的攻击，并将其标记在 *Dynamic Code Evaluation: JNDI Reference Injection 类别下。*
此外，升级后的 Log4j 支持涵盖以下命名空间的最新 Log4j 版本：

- org.apache.logging.log4j

支持还扩大了对以下漏洞类别的覆盖范围：

- Code Correctness: Stack Exhaustion
- Dynamic Code Evaluation: JNDI Reference Injection
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak

Azure Functions（Python，支持的版本：3.10.x）

Azure Functions 是一种无服务器云计算解决方案，可以执行代码以响应预定义事件，例如 API 调用、数据库事务或管理其他 Azure 服务中的消息队列。在此版本中，我们扩展了对 Azure Functions 的支持，以涵盖 Python 中的 HTTP 触发器函数。HTTP 触发器有助于通过 HTTP 请求调用函数，并可用于构建无服务器 API 以及响应 Webhook。
支持涵盖了以下类别：

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- Privacy Violation
- System Information Leak: External

GraphQL 支持：Python Graphene（支持的版本：3.0.0）

此版本增加了对 Python Graphene 的初始 GraphQL 服务器支持。GraphQL 是一个由 Facebook 开发的开源项目，具有用于 API 的强类型查询语言和服务器端运行时引擎。自 2015 年以来，GraphQL 一直采用开放标准，目前支持二十多种编程语言。Graphene 是一款适用于 Python 应用程序的受欢迎 GraphQL 服务器框架。此版本增加了以下两个类别来检测使用 Graphene 开发的 GraphQL API 中的漏洞：

- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled

Kotlin 更新（支持的版本：1.5）

Kotlin 是一种具有 Java 互操作性的通用静态类型语言。此版本更新了对标准库 API 的支持，该 API 在 Kotlin 1.5 中引入并针对 Java 虚拟机 (JVM)。

Sequelize（支持的版本：6.17）

Sequelize 是一款基于 Promise 的对象关系映射 (ORM) 工具，旨在简化在 Node.js 应用程序中使用许多热门 SQL 方言的方式。支持涵盖了以下类别：

- Access Control: Database
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- SQL Injection

在 HTML 中引用的文件不安全

在网页中对第三方站点的所有引用都应通过安全连接进行，因此该版本在 HTML 文件中增加了对以下新类别的支持：

- Dynamic Code Evaluation: Insecure Transport
- Insecure Transport: External Link

共享密码数据库检测

密码数据库是用于安全存储密码的文件或文件集。密码数据库通常使用主密码或主密钥进行加密。但是，在应用程序的整个开发生命周期内不应利用密码数据库来持续使用密码。在此版本中，我们将存在的这类数据库报告为：*Password Management: Shared Password Database*。支持的密码数据库包括：

- KeePass
- 1Password
- Password Safe
- MacOS Keychain
- Gnome Keyring
- KDE KWallet

云基础设施即代码

此版本扩展了对云基础设施即代码 (IaC) 的支持。基础设施即代码是指通过代码管理和配置计算资源的过程，而非手动过程。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。

支持的其他类别包括：

- Ansible Bad Practices: CloudWatch Log Group Retention Unspecified
- Ansible Bad Practices: Unrestricted AWS Lambda Principal
- Ansible Bad Practices: User-Bound AWS IAM Policy
- Ansible Misconfiguration: Azure Monitor Missing Administrative Events
- Insecure Storage: Missing EC2 AMI Encryption
- Insecure Storage: Missing EFS Encryption
- Insecure Storage: Missing Kinesis Stream Encryption
- Insecure Transport: Azure App Service
- Insecure Transport: Azure Storage
- Kubernetes Bad Practices: Automated iptables Management Disabled
- Kubernetes Bad Practices: Kernel Defaults Overridden
- Kubernetes Bad Practices: Kubelet Streaming Connection Timeout Disabled
- Kubernetes Bad Practices: Missing NodeRestriction Admission Controller
- Kubernetes Bad Practices: Missing PodSecurityPolicy Admission Controller
- Kubernetes Bad Practices: Missing Security Context
- Kubernetes Bad Practices: Missing SecurityContextDeny Admission Controller
- Kubernetes Bad Practices: Missing ServiceAccount Admission Controller
- Kubernetes Bad Practices: Service Account Token Automounted
- Kubernetes Bad Practices: Shared Service Account Credentials
- Kubernetes Misconfiguration: Insecure etcd Client Transport
- Kubernetes Misconfiguration: Insecure etcd Peer Transport
- Kubernetes Misconfiguration: Missing Kubelet Certificate Authentication
- Kubernetes Misconfiguration: Missing Service Account Token Authentication
- Kubernetes Misconfiguration: Weak SSL Certificate for Kubelet

外部加密密钥和捆绑包

加密密钥可以存储在与源代码不同的文件中，但在版本控制系统中持续存在。此外，加密密钥也可以存储在加密捆绑包中，该捆绑包是一个用于存储加密对象（例如证书和加密密钥）的文件。在此版本中，我们将存在的这类文件报告为：*Key Management: Hardcoded Encryption Key*。支持的加密捆绑包和密钥文件包括：

- Public-Key Cryptography Standards #12 KeyStore
- Java KeyStore（Oracle 的 KeyStore 格式）
- Ruby On Rails 主密钥
- PuTTY 私钥
- Microsoft BitLocker 解密密钥

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：

Insecure Transport: Weak SSL Protocol

安全套接层 (SSL) 和传输层安全 (TLS) 提供了通过网络保护数据的机制。在此版本中，我们更新了对 *Insecure Transport: Weak SSL Protocol* 的支持。除了标记使用的任何 SSL 版本之外，自此版本开始，我们还将标记使用的 TLS 版本 1.0 或 1.1。

Insecure Transport: Weak SSL Cipher

密码套件指定与安全套接层 (SSL) 或传输层安全 (TLS) 配合使用的加密算法。先前由 Fortify WebInspect 报告 *Insecure Transport: Weak SSL Cipher* 结果，现在 Fortify Static Code Analyzer (SCA) 也报告此结果。

Weak Cryptographic Signature

数字签名是一种用于确定数字消息的真实性和完整性的技术。数字签名算法 (DSA) 现已过时，不应再使用。此版本支持在 Java、Ruby 和 PHP 中使用 DSA 时标记 *Weak Cryptographic Signature*。

对 Node 进行了细微改进

我们改进了对 Node.js 包的支持，包括“net”、“http”、“https”和“os”。客户会发现有关 *Cross-Site Scripting*、*Server-Side Request Forgery* 和 *System Information Leak* 类别的结果更准确。

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，客户还会发现以下方面的误报也得到进一步消除：

- Credential Management: Hardcoded API Credentials（在识别 GitHub 访问令牌时）
- Java 应用程序中的“Cross-Site Scripting: Content Sniffing”
- “Portability Flaw: Locale Dependent Comparison”的间歇性误报
- “OGNL Expression Injection: Double Evaluation”的间歇性误报
- Password Management: Hardcoded Password（在示例域中设置时，例如 example.com）
- SQL Injection: iBatis Data Map

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：

漏洞支持 Dangerous File Inclusion: Local

Grafana 是一个用于监控和观察的开源平台。Grafana 的某些版本易受 Directory Traversal（标识为 CVE-2021-43798）的攻击。此漏洞允许访问本地文件。攻击者可能会获取服务器上各文件的内容，这可能导致敏感数据泄露以及专有业务逻辑的潜在恢复。此版本包含用于检测 Grafana 中是否存在此漏洞的检查功能。

策略更新 Aggressive Log4Shell[1]

新的 Aggressive Log4Shell 策略已添加到 SecureBase 支持的策略列表中。与现有策略相比，新策略可以执行更准确、更积极和更果断的扫描，以对使用 Log4j 的 Web 应用程序进行全面的安全评估。其中包括扫描易受攻击的 Apache Log4j 库版本中是否存在 *JNDI Reference Injections* 漏洞。

杂项勘误表

在此版本中，我们已继续投入资源来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：

Log4Shell[1]

此版本改进了 Log4Shell 检查，增加对新的 Aggressive Log4Shell 策略的支持，该策略可更准确地扫描易受攻击的 Apache Log4j 库版本中是否存在 *JNDI Reference Injections* 漏洞。

CSRF 更新

此版本改进了 CSRF 检查，可减少漏报并提高结果的准确性。

[1] 使用 *Log4Shell* 检查功能和 *Aggressive Log4Shell* 策略需要安装 WebInspect 21.2.0.117 修补程序或更高版本。

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。

CyberRes Fortify Taxonomy：软件安全错误

请通过 https://vulncat.fortify.com 访问 Fortify Taxonomy 站点，以查看对新增类别支持的说明。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
Software Security Research CyberRes Fortify 高级经理
hoole@microfocus.com
+1 (650) 258-5916

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