Micro Focus

Fortify 软件安全内容

2019 更新 4

2019 年 12 月 13 日

关于 Micro Focus Fortify 软件安全研究

Fortify 软件安全研究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，Micro Focus Fortify 软件安全内容支持 26 种编程语言的 1,018 个漏洞类别，且涵盖的单独 API 超过一百万个。

如需了解详细信息，请访问：https://software.microfocus.com/en-us/software/security-research

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（2019.4.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）和 Fortify Premium Content 等软件的更新。

Micro Focus Fortify Secure Coding Rulepack [SCA]

这次发行的 Fortify Secure Coding Rulepack 可以检测 26 种编程语言的 807 个不同漏洞类别，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：

Go 初始支持[1]

Go 初始支持。 Go 是一种由 Google™ 设计的静态类型的开源语言，旨在轻松构建简单、可靠和高效的软件。 Go 在语法上类似于 C 语言，但具有内存安全机制、垃圾回收和结构类型。 此更新涵盖 10 个核心标准库命名空间，并支持以下 34 个类别：

- Access Control:Database
- Command Injection
- Connection String Parameter Pollution
- Cookie Security:Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security:Overly Broad Domain
- Cookie Security:Overly Broad Path
- Cross-Site Scripting:Persistent
- Cross-Site Scripting:Poor Validation
- Cross-Site Scripting:Reflected
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: MIME Sniffing
- Insecure Transport
- Key Management:Empty Encryption Key
- Key Management:Hardcoded Encryption Key
- Key Management:Null Encryption Key
- Open Redirect
- Password Management
- Password Management:Empty Password
- Password Management:Hardcoded Password
- Password Management:Null Password
- Password Management: Weak Cryptography
- Path Manipulation
- Path Manipulation:Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- SQL Injection
- System Information Leak:External
- System Information Leak:Internal
- Weak Encryption
- Weak Encryption:Insufficient Key Size

[1] 需要 SCA v19.2.0 或更高版本。

Spring Security

Spring Security 是一个身份验证和访问控制框架，还提供额外的安全层，例如安全标头，它提供针对会话固定、点击劫持和跨网站请求伪造等攻击的额外保护。 它是保护基于 Spring 的应用程序的实际标准。 此更新包括对以下 21 个类别的支持（直到版本 5.2.1）：

- Cookie Security:Cookie not Sent Over SSL
- Cookie Security:Overly Broad Domain
- Cross-Site Request Forgery
- Header Manipulation
- HTML5:Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Missing Content Security Policy
- HTML5:Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5:Overly Permissive Referrer-Policy
- Insecure Transport:HSTS Does Not Include Subdomains
- Insecure Transport:HSTS not Set
- Insecure Transport:Insufficient HSTS Expiration Time
- Password Management
- Password Management:Empty Password
- Password Management:Hardcoded Password
- Password Management:Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- Session Fixation
- System Information Leak

此外，还引入了以下 7 个新的漏洞类型：

- HTML5: Missing Framing Protection
- HTML5: Unenforced Content Security Policy
- Spring Security Misconfiguration: Default Permit
- Spring Security Misconfiguration: Disabled Security Headers
- Spring Security Misconfiguration: Incorrect Request Matcher Type
- Spring Security Misconfiguration: Lack of Fallback Check
- Spring Security Misconfiguration: Overly Permissive Firewall Policy

Spring Boot

Spring Boot 创建独立的 Spring 应用程序，并尽可能自动配置 Spring 和第三方库。 它还提供生产就绪功能，例如指标、运行状况检查和外部化配置。 除了以前支持的类别，此更新还包括对以下其他 9 个类别的支持（直到版本 2.2.1）：

- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Overly Broad Session Cookie Domain
- Cookie Security: Overly Broad Session Cookie Path
- Cookie Security: Persistent Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Password Management: Empty Password in Configuration File
- Insecure Transport
- Insecure Transport:Server Identity Verification Disabled
- System Information Leak:External

此外，虽然以前的 Rulepack 只支持 Properties 配置文件和 Maven 构建系统，但此版本还包括对 YAML 配置文件和 Gradle 的支持。

Java 12[2]

支持 Java 12 中的新 API。当使用新的 Java 12 语法（例如新的 Switch 语句）时，这些规则需要 SCA 版本 19.1 或更高版本。

JSTL XML 库

JavaServer Pages (JSP) 标准标记库 (JSTL) 是一个库，它提供了一种以 JSP 为中心的操作和创建 XML 文档的方法。 现在，支持覆盖了 JSTL v1.1 的以下类别：

- XSLT Injection
- XML External Entity Injection
- Privacy Violation
- System Information Leak:External

OpenXML SDK .NET 改进

对 OpenXML SDK v2.9.0 的更新支持包括对 3 个附加类别的支持：

- Access Control:Database
- Connection String Parameter Pollution
- SQL Injection

React-Router 支持

React Router 是一组导航组件，它们以声明的方式与应用程序组合在一起。 无论您是要为 Web 应用程序提供可添加书签的 URL，还是要以一种可组合的方式在 React 中导航，React Router 都可以在 React 渲染的任何地方工作。 React-Router 5.1.2 支持的类别包括：

- Open Redirect
- Privacy Violation
- System Information Leak:External

2019 CWE Top 25

与称为 SANS Top 25 的时候相比，Common Weakness Enumeration (CWE) Top 25 从根本上改变了确定漏洞的方式。9 月发布的新 Top 25 是使用启发式公式确定的，该公式可规范化过去两年中向国家漏洞数据库 (NVD) 报告的漏洞的频率和严重程度。 为了支持要对 NVD 中最常报告的关键漏洞确定审计优先次序的客户，我们增加了 Micro Focus Fortify Taxonomy 与 CWE Top 25 2019 版本之间的关联。

DISA STIG 4.10

为了向联邦客户提供合规性方面的支持，我们增加了 Micro Focus Fortify Taxonomy 与美国国防信息系统局 (DISA) 应用安全与开发 STIG 版本 4.10 之间的关联。

[2] 需要 SCA v19.2.0 或更高版本。

其他勘误表

在此版本中，我们继续投入资源，以确保我们能够减少误报问题的数量，并提高客户审计问题的能力。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：

- 不安全的反序列化一致性： 以前，某些规则仅在信息来自浏览器时才会标记。 已解决此问题，可在其他可能的情况下进行标记。
- 描述参考已验证： 某些参考材料已过期或指向无效链接。 这些实例现已修复，并已使用适当的参考。

Micro Focus 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

SSO Bad Practices: Authentication Token Replay

在单点登录过程中交换的身份验证令牌容易受到重播攻击，并使攻击者能够假冒有效用户来获得对服务的未授权访问权限。 此版本包括一项检查，该检查使用 SAML 协议对 Windows 身份框架和服务提供商执行重播攻击。

Cache Management: Headers

HTTP Vary 响应标头包含 HTTP 标头的列表，用于确定应对传入请求的正确缓存响应。 Vary 标头中缺少“Origin”会使应用程序同时面对客户端和服务器端缓存中毒攻击，特别是在发出跨源请求时。 此版本包括一项检查，以检测 Vary 标头值中何时出现缺少“Origin”标头的情况。

HTML5: CORS Functionality Abuse

如果允许来自空源“Origin: null”的 CORS 请求， 则可能会危及系统安全性，使应用程序容易遭到数据窃取。 此版本包括一项检查，以检测服务器响应中的 Access-Control-Allow-Origin CORS 标头中是否存在“null”值。

Insecure Deployment: HTTP Request Smuggling[3]

HTTP Request Smuggling 漏洞是由于前端和后端服务器在解析不兼容的 HTTP 标头时存在差异而引起的。 通过提供由不同服务器解释为不同长度的请求，攻击者可能会毒害后端 TCP/TLS 套接字，并将任意数据预置到下一个请求中，或者在前端服务器不知道的情况下将其他请求偷运到后端服务器。此版本包括用于检测此漏洞的检查功能。

[3]Insecure Deployment: HTTP Request Smuggling 检查需要 WebInspect v19.2.0 或更高版本。

Header Manipulation[4]

此版本中已增强现有的 Header Manipulation 检查，除了现有的 CRLF 攻击之外，还包括回车(“CR”)和换行(“LF”)攻击。

合规性报告

DISA STIG 4.10

为了在合规性方面为我们的联邦客户提供支持，此版本包含 WebInspect 检查与最新版美国国防信息系统局应用安全与开发 STIG 版本 4.10 之间的关联。

策略更新

DISA STIG 4.10

在 WebInspect SecureBase 内现有的支持策略列表中，已添加为涵盖与 DISA STIG 4.10 相关的检查而自定义的策略。

Micro Focus 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。

DISA STIG 4.10 和 2019 CWE Top 25

为了配合新关联，此版本还包含附带 DISA STIG 4.10 和 2019 CWE Top 25 支持的 Fortify Software Security Center 新报告包，您可以从 Fortify 客户支持门户下的 Premium Content 下载该报告包。

Micro Focus 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描述，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 Micro Focus Fortify 支持门户获取此更新内容。

[4] Header Manipulation 增强功能需要 WebInspect v19.2.0 或更高版本。

联系 Fortify 技术支持
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

联系 SSR
Alexander M. Hoole
软件安全研究团队经理
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

2019 年 12 月 13 日