Micro Focus
Fortify 软件安全内容

2020 更新 4
2020 年 12 月 18 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 27 种编程语言的 1,039 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/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（2020.4.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）和 Fortify Premium Content 的更新。

Micro Focus Fortify Secure Coding Rulepack [SCA]

这次发行的 Fortify Secure Coding Rulepack 可以检测 27 种编程语言的 817 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：

Dapper 支持（版本 2.0.78）

支持 Dapper 对象关系映射 (ORM)。Dapper 用于通过扩展 .NET IDdbConnection 接口将本机查询输出映射到强类型 C# 对象。新增支持将 Dapper 视为用户控制数据的来源，并将其视为以下类别的触发器：

- Access Control: Database
- SQL Injection

Kotlin 标准库更新（版本 1.3）

扩展了对 Kotlin 标准库的支持，包括以下软件包的覆盖范围：

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull（版本 1）

支持 XML Pull 软件包在 Android 上的实现。XML Pull 是一个简单的流式 API，用于解析和序列化 XML 文件，其中应用程序控制解析（可以中断和恢复）。支持的类别包括：

- XML Entity Expansion Injection
- XML Injection

AIOPG（版本 1.0.0）[1]

支持 Python aiopg 库。Aiopg 提供一种异步方式来连接到 PostgreSQL 数据库。支持的类别包括：

- Access Control: Database
- Password Management
- Password Management: Empty Password

[1] 全面检测与 aiopg 相关的问题取决于对 SCA 的未来改进，该改进与 'async with' 相关。

- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- SQL Injection

JavaScript Promises

- 改进了对数据流分析的 JavaScript Promises 支持。

Azure Resource Management 模板

对 Azure Resource Management (ARM) 模板的初始支持。ARM 模板用于实现基础架构，作为 Azure 解决方案的代码。ARM 模板为 JSON 文件，采用声明性语法来定义和配置用户项目。支持的类别包括：

- Azure Resource Manager Misconfiguration: HTTPS Not Required
- Azure Resource Manager Misconfiguration: Public Access Allowed

DISA STIG 5.1

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 5.1 之间的关联。

NIST SP 800-53 修订版 5

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 与最新版本的美国国家标准与技术研究院 (NIST) 特别出版物 (SP) 800-53 修订版 5 中的安全和隐私控制之间的关联。涵盖 30 个基本控制，涉及以下控制类别：

- Access Control (AC)
- Audit and Accountability (AU)
- Assessment, Authorization, and Monitoring (CA)
- Configuration Management (CM)
- Identification and Authentication (IA)
- PII Processing and Transparency (PT)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

2020 Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE™) Top 25 于 2019 年引入，取代了 SANS Top 25。2020 CWE Top 25 于 8 月发布，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 2020 CWE Top 25 之间的关联。

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：

SCA 17.x 之前版本的弃用
正如 2020.3 发行公告中所述，这将是支持 SCA 17.x 之前版本的最后一个规则包版本。对于此版本，SCA 17.x 之前的版本将不加载最新的规则包。使用 SCA 17.x 之前的版本的客户必须对规则包进行降级或升级 SCA 版本。

对于以后的版本，我们将支持 SCA 的最后四个主要版本。

映射的弃用
软件安全研究团队多年来基于 Fortify 类别以及外部标准和最佳实践不断创建各种映射。因此，我们现在已拥有大量支持不同标准的版本，尽管许多旧版本将不再使用。

因此，我们现在已经将以下标准标记为“过时”：

- 支付卡行业数据安全标准 (PCI) 1.1
- 支付卡行业数据安全标准 (PCI) 1.2
- 支付卡行业数据安全标准 (PCI) 2.0
- 支付卡行业数据安全标准 (PCI) 3.0
- 支付卡行业数据安全标准 (PCI) 3.1
- 支付卡行业数据安全标准 (PCI) 3.2
- 安全技术实施指南 (STIG) 4.1
- 安全技术实施指南 (STIG) 4.2
- 安全技术实施指南 (STIG) 4.3
- 安全技术实施指南 (STIG) 4.4
- 安全技术实施指南 (STIG) 4.5
- 安全技术实施指南 (STIG) 4.6
- 安全技术实施指南 (STIG) 4.7
- 安全技术实施指南 (STIG) 4.8

此更改意味着自 20.2 版本起的 Fortify SCA 应用程序默认将不会显示这些旧映射。

如果需要检查这些旧版本的合规性，您必须更改映射，将 *obsolete* 属性设置为“false”，或者完全删除该属性。

误报改善：

我们继续听取客户的意见，并努力改善误报率。在此版本中，我们致力于下列工作以减少误报次数：

- 消除了配置文件中存在保护时出现的 HTTP 谓词篡改误报
- 消除了在 .NET 中使用 JSONIGNORE 属性时出现的大量赋值误报
- 消除了在 URLSessionConfiguration 对象中显式禁用缓存时出现的 Insecure Storage: HTTP Response Cache Leak 误报
- 消除了来自 URLRequest 的 Swift Privacy Violation: Http Get 误报
- 消除了 Python 中的 Poor Logging Practice: Use of a System Output Stream 重复问题
- 消除了使用其他 Apache Commons closeQuietly 变体时的 Unreleased Resource 问题

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

Weak Cryptographic Signature: 可预测的密钥

通常使用 HMAC 签名确保 JSON Web Token 有效负载的完整性。然而，如果 HMAC 算法使用弱机密，恶意用户可以通过暴力手段获取密钥，并使用任意有效负载对 JWT 进行重新签名。此版本包含一项检查，用于确定是否使用了来自常用机密的字符串来对 JWT 令牌进行签名。

Password Management: 弱密码策略

可确保用户创建强密码的密码策略对部署安全的网站十分关键。应对密码进行验证，以确保它们不是常用密码，且密码字符串应符合 NIST 800-53、NIST 800118 和 OWASP 规定的准则。此版

本包含一项新的检查，用于检测登录宏中配置的密码是否为常用密码。此版本还包括对弱密码策略检查的更新，以符合上述 NIST 标准和 OWASP 指南中关于密码强度的修订指南。

Cache Management: Web 缓存中毒

当用户首次访问网站时，Web 缓存会存储页面的副本。下次用户访问同一页面时，系统会向其提供一个缓存副本。但是，如果这些 Web 缓存存在实施或设计缺陷，例如接受带有请求体的 GET 请求（如 fat GET 请求或未知输入），则它们很容易受到 Web 缓存中毒的影响。Web 缓存中毒是攻击者用来缓存合法用户请求的恶意响应的高级技术。此版本包含的检查用于确定网站是否容易受到通过不明标头和 fat GET 请求的 Web 缓存中毒的攻击。

合规性报告

DISA STIG 5.1

为了向我们的联邦客户提供合规性支持，此版本包含 WebInspect 检查与最新版本的美国国防信息系统局应用安全与开发 STIG 版本 5.1 之间的关联。

NIST SP 800-53 修订版 5

为了向我们的联邦客户提供合规性方面的支持，此版本包含 WebInspect 检查与最新版本的美国国家标准与技术研究院 (NIST) 特殊出版物 (SP) 800-53 修订版 5 中的控制之间的关联。

2020 Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE™) Top 25 于 2019 年引入，取代了 SANS Top 25。2020 CWE Top 25 于 8 月发布，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。此 SecureBase 更新包括到这些 CWE 类别的映射。我们所包括的检查，要么直接映射到由 CWE Top 25 标识的类别，要么映射到通过 "ChildOf" 关系与 Top 25 中 CWE-ID 关联的 CWE-ID。

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：

- 重新设计了 HTTP Request Smuggling 检查，以减少误报，提高效率，并提高其结果的准确性。检查 ID 11621 不再使用基于时间的方法进行漏洞验证。

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 5.1、NIST SP 800-53 修订版 5 和 2020 CWE Top 25

为了配合新关联，此版本还包含附带 DISA STIG 5.1、NIST SP 800-53 修订版 5 和 2020 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 Micro Focus Fortify 支持门户获取此更新内容。

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

2020 年 12 月 18 日