Micro Focus

Fortify 软件安全内容

2021 更新 1

2021 年 3 月 26 日

关于 Micro Focus 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，Micro Focus Fortify 软件安全内容支持 27 种编程语言的 1,038 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 Software Security Research (SSR) 团队荣幸地宣布，我们即将推出 Fortify Secure Coding Rulepack（2021.1.0 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 816 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：

Micro Focus Visual COBOL 支持（版本 6）[1]

该版本增加了对 Micro Focus Visual COBOL 版本 6 的支持。尤其是，该版本包含了对 Micro Focus COBOL Runtime System (RTS) 的支持，并且扩展了对已支持的 COBOL Path Manipulation 类别和以下附加类别的支持：

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

Android 11

我们一直支持最新版的 Android（API 版本 30），现在涵盖了以下命名空间：

- android.accounts
- android.app
- android.database
- android.database.sqlite

用户应该会发现，Android 应用程序建模水平的提高总体上完善了结果，并在 *SQL Injection* 和 *Access Control: Database* 上有额外的收获。

iOS 更新

我们始终致力于改进对 iOS 的支持，增加了以下类的全新 Swift 规则：

- Foundation.NSCache
- Foundation.URLFileProtection

用户应该会发现，与 Data Protection 和 Privacy Violation 相关的结果得以改进，同时对其他漏洞类型和框架也进行了全面改进（请参阅“杂项勘误表 - iOS 漏洞修复”）。

Angular 支持更新（版本 11.2.3）

该版本将我们的 Angular 支持更新到 11.2.3。特别是我们识别了浏览器中用户控制信息的新来源，这可能导致很多类别触发之前未曾触发的事件。

[1] 需要 SCA 21.1 或更高版本。

Apache Commons 更新

Apache Commons 提供可重用的 Java 组件。在该版本中，SSR 更新了对以下组件的支持：

- beanutils (1.9.4)
- collections4 (4.4)
- dbutils (1.7)
- fileupload (1.4)
- lang (3.11)
- math (3.6.1)
- io (2.8.0)
- text (1.9)

这些更新改进了使用这些组件对应用程序的建模，能够识别对 Log Forging 和 JSON Injection 等类别的防护，并且能够识别以下漏洞类型可能出现的新区域：

- Access Control: Database
- Denial of Service
- Insecure Randomness: User-Controlled Seed
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak（变体）

Python（版本 3.9）

更新了对最新版 Python 的支持，改进了对核心语言 API 的建模。

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：

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：

- *Java 和 Kotlin 应用程序中的 Code Correctness: Erroneous Class Compare*
- *Dynamic Code Evaluation: Code Injection* 问题从 Python 3 扫描中移除
- *Key Management* 问题已得到改进，移除了所有语言的误报
- *Cross-Site Scripting: DOM* 问题（与 jQuery 相关）现已正确归类为 *Cross-Site Scripting: Self*（当来自输入框时）。
- 移除了配置文件中匹配非密码内容时的 *Password Management* 问题
- 对照本地化数据时改进了 *Password Management* 误报
- 移除了 Java Spring 应用程序中无关函数的 *XML External Entity Injections* 结果。
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* 现在将更多谓词视为安全（PATCH、DELETE、PUT）。

iOS 漏洞修复：
由于分析改进，因此要对规则进行更新。这会使用户发现以下漏洞类型有所改进：
- 输入拦截：允许键盘扩展
- Privacy Violation: HTTP Get
- Privacy Violation: 键盘缓存
- Privacy Violation: 屏幕缓存
- Privacy Violation: Shoulder Surfing

多个框架也有小幅更新，提高了准确性：Foundation、UIKit、WebKit、HealthKit、WatchKit、MessageUI、CoreLocation、CoreData。

移除类别：
以下类别已在该版本中移除，以提高结果的相关性：
- Privilege Management: Android Network

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

OGNL Expression Injection: Struts 2

通过 CVE-2019-0231 和 CVE-2020-17530 识别到的关键 OGNL Expression Language Injection 漏洞影响 Struts 版本 2.0 到 2.5.25。利用这些漏洞可能会导致在服务器上执行任意远程代码。此版本包括一项检查功能，用于检测使用 Struts 2 的 Web 应用程序中是否存在这些漏洞。

WAF Detection[2]

此版本包括“WAF Detection”检查功能，此功能可标记在扫描期间检测到 Web 应用程序防火墙时的信息结果。这些结果表明扫描质量可能会受到影响，因为扫描请求在到达应用程序之前便遭到阻止。

Hacker Level Insights[2]

Hacker Level Insights 为开发人员和安全专业人员提供了与其应用程序的总体安全态势相关的上下文。此版本包括一项检查功能，用于标记在扫描期间在应用程序中检测到的库。尽管这些结果未必表示存在安全漏洞，但需要注意的是，攻击者通常对这些类型的目标进行勘测，试图识别已知的漏洞或模式。

[2] 需要 WebInspect 21.1 或更高版本。

策略更新

NIST SP 800-53 修订版 5

在 WebInspect SecureBase 的支持策略列表中，添加了一项自定义策略以纳入与 NIST SP 800-53 修订版 5 相关的检查。

CWE Top 25 2020

在 WebInspect SecureBase 的支持策略列表中，添加了一项自定义策略以纳入与 CWE Top 25 2020 相关的检查。

DISA STIG 5.1

在 WebInspect SecureBase 的支持策略列表中，添加了一项自定义策略以纳入与 DISA STIG 5.1 相关的检查。

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：

Web 缓存中毒
此版本包括对 *Web 缓存中毒：不明标头* 的更新检查功能。用户现在可以添加他们怀疑为缓存密钥一部分的自定义标头。

不安全的 SpringBoot Actuator
此版本包括对检测非特权用户可用的敏感 Spring Boot Actuator 的更新检查功能，该检查可提供更精确的结果。

XSS 改进
此版本包括对 Vue 3 和 Angular JS 1.5.9 及更高版本改进的 XSS 攻击检查功能。

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。

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

2021 年 3 月 26 日