Micro Focus

Fortify 软件安全内容

2019 更新 2

2019 年 6 月 28 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 25 种编程语言的 1,005 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（2019.2.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）、Fortify Application Defender 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 25 种编程语言的 799 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：

.NET 更新

支持 .NET Framework 4.7.1 版和 4.7.2 版中引入的 API 新增功能。更新内容包括对 .NET Standard 2.0 和 .NET Core 2.0 的规则支持，其涵盖与 .NET Framework 所支持的相同类别。.NET Framework 更新版本的规则包括对以下类别的增强支持：

- Header Manipulation:Cookies
- Insecure SSL:Server Identity Verification Disabled
- Insecure Transport:Weak SSL Protocol
- Weak Cryptographic Hash
- Weak Cryptographic Signature:Insufficient Key Size
- Weak Encryption

Realm 数据库

Realm 数据库是一种专门为移动应用程序设计的开放源代码轻量级数据库，现在支持 iOS（Swift 和 Objective-C）和 Android (Java)。支持的类别如下：

- Access Control:Database
- Key Management:Empty Encryption Key
- Key Management:Hardcoded Encryption Key
- Key Management:Null Encryption Key
- Path Manipulation

此外，还支持两个新类别：

- Insecure Storage:Missing Database Encryption
- NoSQL Injection:Realm

Python urllib3

Python urllib3 库是一种常用的强大 HTTP 客户端，现已受支持。涵盖的类别如下：

- Header Manipulation
- Insecure SSL:Server Identity Verification Disabled
- Password Management
- Password Management:Empty Password
- Password Management:Hardcoded Password
- Password Management:Null Password
- Password Management:Weak Cryptography
- Server-Side Request Forgery

Java SE 10 和 11 更新

Java SE 的覆盖范围已经扩展到版本 10 和 11，包括对新 HTTP 客户端 API 的支持。

Cross-Site Scripting:SOP Bypass

JavaScript 和 TypeScript 中对新类别“Cross-Site Scripting:SOP Bypass”的支持。此新类别涵盖一种特定情况，其中漏洞使攻击者能够绕过同源策略 (SOP) 来实现 Cross-Site Scripting 攻击。

PCI SSF 1.0

为了对我们的电子商务和金融服务客户提供合规性支持，此版本支持 Micro Focus Fortify Taxonomy 类别与在支付卡行业 (PCI) 安全软件标准 (SSS)（新的软件安全框架 (SSF) 1.0 版的一部分）中定义的新“安全软件要求和评估程序”中指定的控制目标之间的关联。新标准旨在最终将 PCI 数据安全标准 (DSS) 替换为新的支付申请 (PA) DSS 标准（提交截止时间为 2020 年年中）以及对现有 PA-DSS（将于 2022 年到期）的更改。

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。客户还会看到与以下项相关的报告问题的更改：

Log Forging

减少所有语言的误报，因为可以更准确地识别将删除新行的 API，以防止出现 Log Forging 和 Log Forging（调试）问题。

Unreleased Resource:Database

在 Java 中，如果先关闭创建 ResultSet 的语句，则算法无法正确标识此 ResultSet 是否自动关闭。现已删除相关误报。

Unsafe JNI 和 Unsafe JSNI

已升级到 SCA v19.1.x 的客户可能已观察到 Java 应用程序中出现了大量新的“Unsafe JNI”和“Unsafe JSNI”问题。这是因为引擎得到改进。这意味着大量 API 标记客户无法控制修复情况。现在已经纠正此情况，以便 SCA 只标记用户可以控制源代码的 API。除了这些问题减少，客户可能还会注意到“Access Control:SecurityManager Bypass”问题也在减少。

Dynamic Code Evaluation 和 Lambda 上的其他接收器

在 JavaScript 应用程序中，由 Lambda 调用引起的问题可能会导致混淆的结果。一个常见的示例是 setTimeout()。这些无关的问题现在都已删除，尽管在某些情况下，这些问题仍然可能发生，但我们正在积极努力地降低其发生频率。仅当使用 SCA v18.20 或更高版本时才会注意到此频率已降低。

Cross-Site Scripting:Content Sniffing 支持

以前，当响应的 content-type 已阻止浏览器处理 HTML/JS 内容（例如 application/json）时，SCA 报告会 Cross-Site Scripting 问题。之所以这样做，是因为 Web 应用程序的用户可能在使用较低版本的浏览器，这些浏览器容易遭受 content-sniffing 攻击。在此版本中，我们已修改这些问题，使其报告为“Cross-Site Scripting:Content Sniffing”。这使审计人员和开发人员能够快速识

别它们，并将其与更严重的 Cross-Site Scripting 情况区分开来。Java Rulepack 中的 Spring Framework 和 JAX-RS 都支持此新类别。

根据污点降低 Fortify 优先级

以前，对于源自 HTTP 请求参数和源自系统环境变量的 SQL Injection，SCA 报告的严重性相同。我们了解，攻击者控制系统变量的可能性非常低，或者至少低于控制请求参数的可能性。基于这一点，我们已经降低某些情况中问题的 Fortify 优先级值，但是从此版本起，SCA 将更一致地应用污点源作为计算问题的 Fortify 优先级值时的新因素。

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

WebSocket 更新[1]

此版本包含的增强功能可检测 WebSocket 流量中的 Information Leak 和 Unsafe Deserialization（对于 .NET）漏洞。具体而言，增强了以下类别以支持 WebSocket：

- Dynamic Code Evaluation:Unsafe Deserialization
- Poor Error Handling:Unhandled Exception
- Privacy Violation
- Privacy Violation:Credit Card Number
- Privacy Violation:National ID Disclosure
- Privacy Violation:Social Security Number
- System Information Leak:Internal IP

安全响应标头配置更新

服务器可以使用一组 HTTP 响应标头来提供可增强应用程序安全性的浏览器配置。这些标头可视为一种深入防御机制，它们在经过设置后可以充分防止漏洞。此版本包含对以下标头和相关类别的增强支持：

- Cache-Control
  - Cache Management:Insecure Policy
- Content-Security-Policy
  - HTML5:Missing Content Security Policy
  - HTML5:Deprecated Content Security Policy
  - HTML5:Misconfigured Content Security Policy
- X-Content-Type-Options
  - Web Server Misconfiguration:Insecure Content-Type
- X-XSS-Protection
  - HTML5:Cross-Site Scripting Protection

[1]WebSocket 更新需要 WebInspect 19.1.0 或更高版本。

Web Server Misconfiguration:Deprecated SSL/TLS Certificate

由 Symantec 证书颁发机构（包括如 Thawte、VeriSign、Equifax、GeoTrust 和 RapidSSL 等 Symantec 拥有的品牌）在 2017 年 12 月 1 日前颁发的所有 SSL/TLS 证书都不受信任，并且不再被 Chrome、Internet Explorer、Firefox 和 Safari 等所有主要浏览器接受。此版本包含的检查功能可用于标记对已弃用 Symantec 证书的使用。

Insecure Deployment:Unpatched Application

Drupal 内容管理系统 (CMS) 中标识为 CVE-2019-6340 的关键 Remote Code Execution 漏洞使远程攻击者能够在服务器上执行任意代码。此版本包括用于检测部署了 Drupal CMS 的应用程序中是否有此漏洞的检查功能。

合规性报告

PCI SSF 1.0

为了对我们的客户提供合规性支持，此版本包括一个新的合规性报告模板，用于将 Micro Focus Fortify Taxonomy 与支付卡行业 (PCI) 安全软件标准 (SSS)（新的软件安全框架 (SSF) 1.0 版的一部分）中定义的新“安全软件要求和评估程序”中指定的控制目标相关联。新标准旨在最终将 PCI 数据安全标准 (DSS) 替换为新的支付申请 (PA) DSS 标准（提交截止时间为 2020 年年中）以及对现有 PA-DSS（将于 2022 年到期）的更改。

策略更新

PCI SSF 1.0

在 WebInspect SecureBase 内现有的支持策略列表中，已添加为纳入与 PCI SSF 1.0 相关的检查而自定义的策略。

其他勘误表

Cache Management:Insecure Policy

增强了检查 ID 11306，以排除对特定 content-type 的 HTML 响应的标记，这些 content-type 在手动验证时通常被审计为误报结果。

Expression Language Injection:Spring

改进了 SecureBase 检查 ID 11579 中的漏洞检测算法的准确性。

Micro Focus Fortify Premium Content

研究团队在我们的核心安全情报产品之外构建、扩展并维护各种资源。

PCI SSF 1.0

除新关联之外，此版本还包含附带 PCI SSF 1.0 支持的 Fortify SSC 新报告包，您可从 Premium Content 下的 Fortify 客户门户下载该报告包。

Micro Focus Fortify Taxonomy：软件安全错误

要访问包含新增类别支持描述的 Fortify Taxonomy 站点，可通过以下网站访问：https://vulncat.fortify.com。对于在旧站点查找最新支持更新的客户，可从 Micro Focus Fortify 支持门户获取该更新内容。

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

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

2019 年 6 月 28 日