软件安全研究发行公告

Micro Focus

Fortify 软件安全内容

2019 更新 1

2019 年 3 月 29 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 999 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（2019.1.0 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 796 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：

Angular 7[1]

支持 7.0.0 及以下版本的 Angular、识别来自浏览器的输入源以及模拟 Angular 在默认情况下执行的安全验证。对 Angular 模板进行建模，以便 Angular 项目支持所有常规 JavaScript 接收器，并且能够查找 Cross-Site Scripting: DOM、Privacy Violation、Dynamic Code Evaluation 问题以及许多其他类别。

AWS Lambda 函数支持

全新的 Amazon Web Services (AWS) Lambda 函数支持 Java 和 Python 语言。该功能支持从 Lambda 触发事件到 Lambda 函数逻辑的数据流，包括 Lambda 连接到 API 网关时遇到的潜在 XSS 问题。

AWS Java SDK v2

新增了对适用于 S3 和 DynamoDB 服务的 AWS Java SDK v2 的支持。包括如下新类别：

- Access Control: ACL Manipulation
- Insecure Storage: S3 Full Anonymous Access
- Insecure Storage: S3 Read ACP Anonymous Access
- Insecure Storage: S3 Read Anonymous Access
- Insecure Storage: S3 Write Anonymous Access
- Insecure Storage: S3 Write ACP Anonymous Access
- NoSQL Injection: DynamoDB

Python Django[1]

更新了对 Python Django Web 框架的支持，包括对 2.1.7 以下版本的支持。更改包括改进了对基于类的视图和关联数据流的支持，以及支持自 Django 1.8 以来引入的 Django 函数/方法。

Apache Wicket[1]

改进了对 Apache Wicket Web 框架的支持，包括对框架版本 6、7 和 8 的支持。

DISA STIG 4.9

为了向我们的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 4.9 之间的关联。

[1]支持 Angular 7、Django 和 Wicket 需要使用 Fortify SCA 19.1.0 或更高版本才能取得最佳结果。

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

Often Misused: File Upload

Blueimp 开发的 jQuery File Upload 小组件容易受到标记为 CVE-2018-9206 的远程代码执行漏洞的攻击。攻击者可以使用该漏洞上传和执行任意 PHP 文件。此版本包括用于检测此漏洞的检查。

SQL Injection

此版本包括 SQL Injection 检查的增强功能，以支持使用 Microsoft Azure SQL 数据库的应用程序。

Sensitive Information Leak: External

此版本包括用于检测 Magento CMS 是否在开发人员模式下运行的检查。开发人员模式应在开发或测试环境中使用。在生产环境中启用开发人员模式可能会将重要的应用程序和系统数据暴露给潜在攻击者，从而带来安全风险。

Cross-Frame Scripting

内容安全策略 *frame-ancestors* 指令标头可以针对 Cross-Frame Scripting 漏洞提供策略保护。该标头将取代当前正在使用的 X-Frame-Options HTTP 标头。 此版本包括现有 Cross-Frame Scripting 检查的增强功能，以支持内容安全策略 frame-ancestors 指令。

Content Management System (CMS) Fingerprinting

此版本包括增强功能，可在 WebInspect 扫描期间通过指纹检测目标服务器上是否存在以下某个 CMS：WordPress、Drupal、Django、Joomla、Liferay、Magento、Sitecore、Sitefinity[2] 和 Umbraco。此时将触发信息检查以报告发现的结果。

合规性报告

DISA STIG 4.9

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防信息系统局应用安全与开发 STIG 版本 4.9 之间的关联。

策略更新

[2]Sitefinity 检测需要使用 WebInspect 19.1.0 或更高版本。

DISA STIG 4.9

在 WebInspect SecureBase 内现有的支持策略列表中，已添加为纳入与 DISA STIG 4.9 相关的检查而自定义的策略。

Micro Focus Fortify Application Defender

Fortify Application Defender 是一个运行时应用程序自我保护 (RASP) 解决方案，可帮助各组织控制和降低自身或第三方应用程序带来的风险。它可以集中查看应用程序使用和滥用情况，还可实时防范对软件漏洞的利用和其他违规现象。对于此版本，Micro Focus Fortify 软件安全研究团队提供了以下功能改进：

OGNL Expression Injection: Struts 2

扩展了对 Apache Struts 2 中的 OGNL Expression Injection 检测的支持，其中涵盖标记为 CVE-2018-11776 的关键 Struts 漏洞。如果使用 Apache Struts 2 版本 2.3.x 至 2.3.34 或版本 2.5.x 至 2.5.16 的应用程序包含的操作结果未使用命名空间或通配符命名空间进行配置，并且在 struts 配置中还将 struts.mapper.alwaysSelectFullNamespace 属性设置为 true，则此类应用程序将允许攻击者执行任意 OGNL 表达式。

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。

DISA STIG 4.9[3]

除新关联之外，此版本还包含附带 DISA STIG 4.9 支持的 Fortify SSC 新报告包，您可从 Premium Content 下的 Fortify 客户支持门户下载该报告包。

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。

[3]支持 DISA STIG 4.9 报告需要使用 Fortify SSC 18.20 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
软件安全研究经理
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

2019 年 3 月 29 日