Fortify 软件安全内容

2021 更新 3
2021 年 9 月 24 日

关于 CyberRes 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、Fortify WebInspect 和 Fortify Application Defender）的安全情报。现在，CyberRes Fortify 软件安全内容支持 27 种编程语言的 1,051 个漏洞类别，且涵盖的单独 API 超过一百万个。

Fortify Software Security Research (SSR) 团队荣幸地宣布，我们即将推出对以下产品的更新：Fortify Secure Coding Rulepacks（2021.3.0 英文版）、Fortify WebInspect SecureBase（可通过 SmartUpdate 获取）和 Fortify Premium Content。

CyberRes Fortify Secure Coding Rulepacks [Static Code Analyzer]

这次发行的 Fortify Secure Coding Rulepacks 可以检测 27 种编程语言的 831 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：

Golang 标准库更新（版本：1.16）

扩展了对 Go 标准库的支持。Go 是一种由 Google 设计的静态类型开源语言，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。此更新涵盖标准库命名空间，并增加了对以下类别的支持：

- Cookie Security：Missing SameSite Attribute
- Cookie Security：Overly Permissive SameSite Attribute
- Go Bad Practices：Leftover Debug Code
- Insecure Randomness：Hardcoded Seed
- Insecure Randomness：User-Controlled Seed
- Insecure Transport：Cipher Suite Downgrade
- Insecure Transport：Weak SSL Protocol
- Often Misused：Privilege Management
- Weak Cryptographic Signature

Android 11 更新（API 级别：30）

Android 平台是专为移动设备设计的开源软件堆栈。Android 的其中一个主要组件是 Java API 框架，该框架会向应用程序开发人员公开各项 Android 功能。此版本扩大了原生 Android 应用程序中的漏洞检测范围，这些应用程序是以利用 Android 的 Java API 框架的 Java 或 Kotlin 语言编写的。经过多次更新 Android 应用程序建模和 API 覆盖率工具，用户应该会发现结果有所改善。而且，此版本还新增了以下权限管理漏洞类别，可为危险的 Android 权限提供指导：

- Privilege Management：Android Activity Recognition
- Privilege Management：Android Calendar
- Privilege Management：Android Call Log
- Privilege Management：Android Camera
- Privilege Management：Android Contacts
- Privilege Management：Android Microphone
- Privilege Management：Android Sensors

iOS 标准库更新（版本：iOS 14）

此版本更新了我们对面向 Swift 和 Objective-C 的 iOS 14 库 API 的支持。这次的更新主要针对于以下框架：

- UIKit
- UserNotification
- SwiftUI
- MessageUI

用户应该会发现我们改进了以下类别：Insecure IPC、Link Injection、Path Manipulation、Privacy Violation、Shoulder Surfing 和 System Information Leak。

Micro Focus Visual COBOL 更新（版本：7.0）

扩展了对 Micro Focus Visual COBOL 版本 7 的支持，以增加对以下两个漏洞类别的支持：

- Integer Overflow
- Race Condition：File System Access

SAPUI5/OpenUI5 支持 [1]（版本：1.93）

SAPUI5 是由 SAP 创建的客户端 JavaScript 框架，该框架与开源 OpenUI5 共用一组核心控件库。此版本提供识别以下漏洞类别的初始支持：

- Cross-Site Scripting：DOM
- Cross-Site Scripting：SAPUI5 Control
- Cross-Site Scripting：Self
- Privacy Violation
- SAPUI5 Misconfiguration：Unsanitized Editor
- System Information Leak：External

JSON 支持 [2]

JavaScript 对象表示法 (JSON) 是一种轻量级数据交换格式。此版本改进了对识别以下 JSON 漏洞类别的支持：

- Password Management：Empty Password
- Password Management：Hardcoded Password
- Password Management：Null Password
- Password Management：Password in Comment[3]

[1] 使用 Static Code Analyzer v21.2.0 或更高版本时，结果应该会得到改善。

[2] 需要使用 Static Code Analyzer v21.1.0 和标记：“-Dcom.fortify.sca.use.json-analyzer=true”。

[3] 需要使用 Static Code Analyzer v21.2.0 或更高版本。自 Static Code Analyzer v21.2.0 版本起，不需要使用任何标记。

Kotlin 标准库更新（版本：1.4.30）

Kotlin 是一种具有 Java 互操作性的通用静态类型语言。此版本更新了对 Kotlin 1.4 中针对 Java 虚拟机 (JVM) 引入的新标准库 API 的支持。

ECMAScript 2021（版本：ECMA-262）

支持 ECMAScript 2021 中引入的新 API。根据 ECMAScript 语言规范的定义，ECMAScript 是一种通用编程语言，以集成到所有现代 Web 浏览器中而为人所熟知。然而，它越来越普遍地用于构建 Web 服务器、移动应用程序和其他类型的传统应用程序。在扫描针对最新 ECMAScript 标准的应用程序时，客户应该会发现数据流有所改善。

2021 Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) 于 2019 年引入，取代了 SANS Top 25。2021 CWE Top 25 于 7 月发布，该列表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) 报告漏洞的频率以及漏洞严重程度。为了支持要对 NVD 中最常报告的关键漏洞确定审核优先次序的客户，我们增加了 CyberRes Fortify Taxonomy 与 2021 CWE Top 25 之间的关联。

杂项勘误表

在此版本中，我们已继续投入资源，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，客户可能还会发现报告的与以下各项相关的问题发生了变化：

弃用版本早于 18.x 的 Static Code Analyzer：

正如您在 2020.4 版本中观察到的，我们将继续支持 Static Code Analyzer 的最后四个主要版本。因此，这将是支持版本早于 18.x 的 Static Code Analyzer 的最后一个规则包版本。对于下一次发行，版本早于 18.x 的 Static Code Analyzer 将不会加载最新的规则包。为此，需要对规则包进行降级或升级 Static Code Analyzer 的版本。
对于未来的发行，我们将继续支持 Static Code Analyzer 的最后四个主要版本。

Java J2EE 改进：

改进了对 *Privacy Violation* 和 *System Information Leak* 类别中 javax.servlet API 的支持。***Android 绑定服务：***

由于我们持续提供 Android 支持，此版本涵盖了 Android 绑定服务。客户可能会遇到源自 Android 绑定服务方法参数的新数据流问题。在该绑定服务中调用方法时，这可能会引入重复的数据流子跟踪过程。

Node.js 中的弱加密散列：

识别 Node.js 应用程序中使用的弱加密散列。

OWASP ASVS 4.0 映射现在包含对级别的支持

为了支持希望能够查询已报告的违反特定 OWASP 应用程序安全验证标准 (ASVS) 应用程序安全验证级别（L1、L2 和 L3）的问题的客户，最新的安全内容已将这些级别添加到映射名称中。客户现在能够在 *OWASP ASVS 4.0* 分组中搜索相关的 *L1*、*L2* 和 *L3* 关键字，以及设计在 Audit Workbench 和 Software Security Center (SSC) 中使用的相关筛选集和筛选模板。

误报改进：

在此版本中，我们会继续致力于消除误报。除了其他改进之外，客户可能还会发现以下方面的误报也得以消除：

- jQuery 代码中的 *Cross-Site Scripting* 误报
- *使用 JsonIgnore 属性的 .NET 应用程序中的 Privacy Violation：Shoulder Surfing*
- 针对只能控制一个数字的 *Path Manipulation* 问题，提高了降低 Fortify 优先级顺序方面的一致性
- 在 Swift 中，我们不再识别属于枚举的密码
- .NET 中出现 *Missing XML Validation* 问题
- Java 项目中出现 *Missing Check against Null*

CyberRes 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

Insecure Deployment：HTTP Request Smuggling

HTTP2 over ClearText 走私（亦称 h2c 走私）攻击取代了传统的 HTTP 请求走私攻击，后者会滥用无法识别 h2c 的前端（例如代理服务器）来创建通往后端系统的隧道。攻击者可以使用此隧道向后端服务器偷偷发送额外请求，而不会被前端服务器察觉。这样攻击者就可以绕过前端上的授权控制并访问后端系统上的受限资源。此版本增加了一项检查，用于检测 h2c 走私攻击能够使用的配置。

Access Control：Missing Authorization Check

GraphQL 自检功能支持查询服务器以获取有关底层架构的信息。自检功能可提供有关查询、类型和字段等元素的详细信息。默认情况下，GraphQL 自检功能通常处于启用状态。未获得适当授权的攻击者可能会滥用此信息以执行各种攻击，例如 SQL Injection 攻击和批处理攻击。此版本增加了一项检查，用于检测启用了自检功能的 GraphQL 端点。

NoSQL Injection：MongoDB

NoSQL 脚本注入漏洞允许攻击者在数据库中注入恶意查询。MongoDB 是一种 NoSQL 数据库，其文档中声明它允许应用程序运行 JavaScript 操作。NoSQL Injection 漏洞非常危险，因为未经身份验证的攻击者可以提取数据或执行 JavaScript 代码。此漏洞可能会导致远程代码执行、机密性降低、应用程序数据完整性以及 Denial of Service (DoS) 攻击。此版本增加了一项检查，用于检测 MongoDB 中是否存在 NoSQL 脚本注入漏洞。

Dynamic Code Evaluation：Unsafe Deserialization

7.0 之前的 ForgeRock AM 服务器和 14.6.4 之前的 OpenAM 服务器中的预授权不安全 Java 反序列化漏洞已被标识为 CVE-2021-35464。攻击者可以利用此漏洞在 jato.pageSession 参数中编写恶意序列化对象，并通过单个请求将其发送到端点“/ccversion/Version”。该漏洞之所以存在，是因为在应用程序中使用了不安全的第三方 Java 库。通常，攻击者可以利用此漏洞在服务器上执行任意代码、滥用应用程序逻辑或发起 Denial of Service (DoS) 攻击。此版本增加了一项检查，用于检测目标 Web 服务器上是否存在此漏洞。

Cross-Site Scripting：DOM[4]

当动态生成的网页显示未经过正确验证的登录信息等用户输入时，将发生 Cross-Site Scripting 攻击，从而使攻击者能够将恶意脚本嵌入到生成的页面中，然后在查看该站点的任何用户的计算机上执行相应脚本。如果出现基于文档对象模型 (DOM) 的 XSS 漏洞，恶意内容将在 DOM 篡改期间执行。如果执行成功，攻击者可能会利用 DOM Cross-Site Scripting 漏洞来篡改或窃取 Cookie、创建可能被误认为是有效用户发出的请求、泄露机密信息或在最终用户系统上执行恶意代码。此版本包含一项新检查，用于检测客户端 URI 片段上是否存在 DOM XSS 漏洞。

Web Server Misconfiguration：Insecure Mapping Directives

如果将 Nginx 配置为在 Web 服务器上执行 PHP，则有时允许将每个以 .php 结尾的 URI 传递给后端 PHP 解释器（例如 FastCGI）。如果请求的完整路径未指向实际存在的文件，则采用这种不安全的 PHP 配置的 Nginx 会将 URL 路径中的文件夹视为要执行的目标文件。攻击者会利用这种错误配置在任何类型的文件（例如图像文件）中执行任意 PHP 代码，前提是可以将这些文件上载到 Web 服务器并进行访问。此版本增加了一项检查，用于检测目标 Web 服务器上是否存在此漏洞。

[4] 需要 WI v21.2.0 或更高版本。

Integer Overflow

从 0.5.6 到 1.13.2（包含在内）的 Nginx 版本容易受到标识为 CVE-2017-7529 的 Integer Overflow 漏洞的攻击。此问题存在于 Nginx 范围过滤器模块中，攻击者可利用该漏洞发送专门编写的请求来获取潜在的敏感信息。此版本增加了一项检查，用于检测目标 Web 服务器上是否存在 CVE-2017-7529 漏洞。

合规性报告

2021 Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) 于 2019 年引入，取代了 SANS Top 25。2021 CWE Top 25 于 7 月发布，该列表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) 报告漏洞的频率以及漏洞严重程度。此 SecureBase 更新包括到这些 CWE 类别的映射。此 SecureBase 更新所包括的检查，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。

策略更新

CWE Top 25 2021

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 2021 相关的检查。

杂项勘误表

在此版本中，我们已继续投入资源，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，客户可能还会发现报告的与以下各项相关的问题发生了变化：

LDAP Injection

此版本改进了 LDAP Injection 检查，可减少误报并提高结果的准确性。

CyberRes 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。

2021 CWE Top 25

除新关联之外，此版本还包含附带 2021 CWE Top 25 支持的 Fortify Software Security Center 新报告包，您可以从 Premium Content 下的 Fortify 客户支持门户下载该报告包。

CyberRes 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 CyberRes Fortify 支持门户获取此更新内容。

联系 Fortify 技术支持

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

联系 SSR

Alexander M. Hoole
Software Security Research 团队高级经理
CyberRes Fortify hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Software Security Research 团队经理
CyberRes Fortify
peter.blay@microfocus.com