Micro Focus

Fortify 软件安全内容

2018 更新 4

2018 年 12 月 14 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 992 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（2018.4.0 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 789 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：

SQLite 和 iOS 改进

扩展了对 Swift、Objective-C、C 和 C++ 编程语言的 SQLite API 支持。 涵盖 16 个现有漏洞类别，包括 SQL Injection、Access Control: Database 以及与密码和密钥管理相关的问题。 与任何类型的数据库进行交互时所产生的编码漏洞，都可能导致敏感信息泄露、意外更改，甚至是数据丢失。 因此，此版本进行了与隐私相关的其他 iOS 改进，涵盖了 Privacy Violation: Heap Inspection for Swift。

Akka HTTP

支持可实施完整的服务器端和客户端 HTTP 堆栈的 Scala Akka HTTP 模块，该模块是基于 Akka Streams 且兼容 Reactive Streams 的工具包。 漏洞类别涵盖 22 个现有漏洞类型。

JAX-RS 改进

修改了对 JAX-RS 最新版及其引用实现 Jersey 的支持。 除了支持 2.1 中新增的功能，此 Rulepack 还支持客户端 API。 受影响的漏洞类别包括 Privacy Violation、Server-Side Request Forgery 和 System Information Leak。 此外，还添加了一个新的漏洞类别，用作 Cross-Site Scripting 的专用子类别，针对使用 XSS 安全内容类型发送响应的情况。 在这种情况下，我们将报告“Cross-Site Scripting: Content Sniffing”问题，因为特定浏览器可能会进行“内容嗅探”并在响应中执行脚本。

Python six

支持“six”Python 库。 Six 是一种 Python 兼容性库，用于支持与 Python 2 和 3 均兼容的代码库（无需进行修改）。 支持的漏洞类别包括：

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak:External
- Unsafe Reflection

DISA STIG 4.8

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 4.8 之间的关联。

PCI DSS 3.2.1

为在合规性领域支持我们的电子商务和金融服务客户，此版本支持 Security Fortify Taxonomy 类别与最新版支付卡行业数据安全标准 3.2.1 版中指定要求之间的关联。

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

LDAP Injection

LDAP Injection 是一种能够利用基于 Web 的应用来发起的攻击，涉及的应用会根据用户输入构建 LDAP 语句。 当应用未能适当地清理用户输入时，就有可能通过类似于 SQL Injection 的技术修改 LDAP 语句。 LDAP Injection 攻击可能会导致对敏感数据进行未经授权的访问。 此版本包括用于标识 Web 应用中的 LDAP Injection 漏洞的检查功能。

Open Redirect

借助 Open Redirect 漏洞，攻击者能够轻松地利用用户信任的已知站点。 根据供应商公告 SA-CORE-2018-006，Drupal 7 和 8 均容易受到该漏洞的攻击。

Drupal Destination Parameter Anonymous Open Redirect

在 Drupal 8 中，如果未能充分清理“destination”参数值，则会遭到利用，进而触发 Open Redirect 以指向攻击者控制的恶意 URL。 此版本包括用于检测此漏洞的检查功能。

Drupal Path Alias Open Redirect

在 Drupal 7 和 Drupal 8 中，攻击者可以利用路径模块中的漏洞来创建、编辑和管理路径别名，这些别名可能会触发 Open Redirect 以指向攻击者控制的恶意 URL。

Access Control: Authorization Bypass

JSON Web Token (JWT) 是一种用来在双方之间传输数据时创建 URL 安全方式的标准。 令牌中的信息通过 HMAC 或 RSA 算法进行数字签名。 但是，此标准也允许在 JWT 中使用“none”作为哈希算法。 接收使用“none”编码的 JWT 的服务器会将所有 JWT 均视为有效，而不会对数据完整性进行任何验证。 恶意用户可能会利用这点来向服务器发送任意数据。 这可能会导致未经授权访问以及系统和用户数据侵害。 此版本包括用于检测 JWT“none”算法身份验证绕过漏洞的检查功能。

Privacy Violation

JSON Web Tokens (JWT) 用于在双方之间传输数据。 如果未能充分加密，敏感数据可能会暴露给未经授权的用户。 此版本包括对现有检查功能进行的更新，用于检测与信用卡号泄露、社会保险号码泄露以及 HTML5 客户端存储内敏感信息存储检测相关的隐私侵权。

Dynamic Code Evaluation:Code Injection

Pivotal 开发的 Spring Framework 容易受到标记为 CVE-2018-1270 的远程代码执行漏洞的攻击。 攻击者可以使用该漏洞将恶意信息发送到暴露的 STOMP over WebSocket 端点，从而实现远程代码执行。 此版本包含用于检测 Spring Framework 中是否有此漏洞的检查功能。 可以通过 WebSocket 策略访问此检查功能。

WebSocket Discovered

此版本包括用于指示扫描的应用中是否存在 WebSocket 的信息检查功能。 此外，该检查功能还会提醒我们的客户考虑使用包含所有 WebSocket 漏洞相关检查的全新 WebSocket 策略对应用进行扫描。

合规性报告

DISA STIG 4.8

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 4.8 之间的关联。

PCI DSS 3.2.1

此版本包括对最新版支付卡行业数据安全标准 (DSS) 合规性模板 3.2.1 版的支持。

策略更新

DISA STIG 4.8

在 WebInspect SecureBase 内现有的支持策略列表中，已添加为纳入与 DISA STIG 4.8 相关的检查而自定义的策略。

WebSocket

全新的 WebSocket 策略会对应用执行 WebSocket 相关漏洞安全评估。

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 4.8[1]

除新关联之外，此版本还包含附带 DISA STIG 4.8 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。

PCI DSS 3.2.1[1]

除新关联之外，此版本还包含附带 PCI DSS 3.2.1 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

[1] Fortify SSC 18.20 版本或更高版本才支持 DISA STIG 4.8 和 PCI DSS 3.2.1 报告。

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

2018 年 12 月 14 日

Micro Focus

Fortify 軟體安全性內容

2018 更新 4

2018 年 12 月 14 日

關於 Micro Focus Fortify 軟體安全性研究

Fortify 軟體安全性研究團隊將尖端研究成果轉為支援 Fortify 產品組合 (包括 Fortify Static Code Analyzer (SCA)、Fortify WebInspect 和 Fortify Application Defender) 的安全情報。 現在，Micro Focus Fortify 軟體安全性內容能夠跨 25 種程式設計語言支援 992 個弱點類別，且涵蓋 100 多萬個單獨 API。

瞭解詳情

https://software.microfocus.com/en-us/software/security-research

Fortify 軟體安全性研究 (SSR) 團隊很高興地宣佈，現已推出以下產品的更新：Fortify Secure Coding Rulepack (英文，2018.4.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)、Fortify Application Defender，以及 Fortify Premium Content。

Micro Focus Fortify Secure Coding Rulepack [SCA]

在本版本中，Fortify Secure Coding Rulepack 能夠跨 25 種程式設計語言偵測 789 種獨特的弱點類別，且涵蓋 100 多萬個單獨 API。總而言之，本版本包含下列項目：

SQLite 和 iOS 改進

擴大了跨 Swift、Objective-C、C 和 C++ 對 SQLite API 的支援。 涵蓋範圍涉及 16 種現有的弱點類別 (包括 SQL Injection、Access Control: Database)，以及與密碼和金鑰管理相關的問題。與任何類型的資料庫互動相關的程式碼編寫弱點可能導致洩漏敏感資訊、意外修改，甚至會導致資料的遺失。 因此，本版本新增了與隱私權相關的 iOS 改進，涵蓋 Privacy Violation: Heap Inspection for Swift。

Akka HTTP

支援 Scala Akka HTTP 模組，Akka HTTP 是以 Akka Streams 為基礎的工具組，符合 Reactive Streams 標準，可實作完整的伺服器端和用戶端 HTTP 堆疊。 弱點類別涵蓋範圍涉及 22 種現有弱點類型。

JAX-RS 改進

修訂了對最新版 JAX-RS 及其參考實作 Jersey 的支援。 除了支援 2.1 中新增的功能外，此 Rulepack 也包括對用戶端 API 的支援。 受影響的弱點類別包括 Privacy Violation、Server-Side Request Forgery 和 System Information Leak。 此外，已針對 Cross-Site Scripting 的專屬子類別新增了弱點類別，使用 XSS 安全的內容類型傳送回應時會導致此弱點。 在這種情況下，我們會報告「Cross-Site Scripting: Content Sniffing」問題，因為特定的瀏覽器可能會執行「內容探查」，並在回應中執行指令碼。

Python six

支援 "six" Python 程式庫。 Six 是 Python 相容性程式庫，旨在不用修改即可支援與 Python 2 和 3 相容的程式碼基底。 支援的弱點類別包括：

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak:External
- Unsafe Reflection

DISA STIG 4.8

為了在合規領域支援我們的聯盟客戶，本版本新增了 Micro Focus Fortify Taxonomy 與 Defense Information Systems Agency (DISA) Application Security and Development STIG 4.8 版之間的關聯性。

PCI DSS 3.2.1

為了在合規領域支援我們的電子商務和財務服務客戶，本版本支援 Security Fortify Taxonomy 類別與最新版本的 Payment Card Industry Data Security Standard 3.2.1 版中所指定要求之間的關聯性。

Micro Focus Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 在檢查成千上萬的弱點的同時，還可透過原則引導使用者透過 SmartUpdate 立即取得以下更新：

弱點支援

LDAP Injection

LDAP Injection 是用來利用網路應用程式發起的攻擊，會基於使用者輸入來建構 LDAP 陳述式。 當應用程式無法正確處理使用者輸入時，可能會透過與 SQL Injection 類似的技術修改 LDAP 陳述式。 LDAP Injection 攻擊可能會導致在未經授權的情況下存取敏感資料。 本版本包含一項檢查，可識別網路應用程式中的 LDAP Injection 弱點。

Open Redirect

Open Redirect 弱點可讓攻擊者輕鬆利用使用者對已知網站的信任。 依據廠商公告 SA-CORE-2018-006，Drupal 7 和 8 易於遭受此弱點的攻擊。

Drupal Destination Parameter Anonymous Open Redirect

在 Drupal 8 中，可利用對 "destination" 參數值的不充分清理，觸發對攻擊者所控制的惡意 URL 的開放式重新導向。 本版本包含一項檢查，可用來偵測此弱點。

Drupal Path Alias Open Redirect

在 Drupal 7 和 Drupal 8 中，路徑模組中的弱點可讓攻擊者建立、編輯和管理路徑別名，從而可能觸發對攻擊者所控制的惡意 URL 的開放式重新導向。

Access Control: Authorization Bypass

JSON Web Token (JWT) 是一項標準，用來在雙方之間傳輸資料時建立安全的 URL 方法。 權杖內的資訊是已使用 HMAC 或 RSA 演算法進行數位簽署的。 但是，此標準還允許使用 "none" 作為 JWT 中的雜湊演算法。 如果伺服器接受 JWT 的編碼中包含 "none"，則會將所有 JWT 視為有效，但不會對資料的完整性進行任何驗證。 惡意使用者可能利用這個弱點，將任意資料傳送至伺服器。 此弱點可能導致未經授權的存取，還會危害系統和使用者資料。 本版本包含一項檢查，可用來偵測 JWT "none" 演算法授權略過弱點。

Privacy Violation

JSON Web Tokens (JWT) 用來在雙方之間傳輸資料。 如果加密不當，可能會將敏感資料暴露給未經授權的使用者。 本版本包括對現有檢查的更新，這些檢查可偵測與信用卡號碼洩漏、身分證號碼洩漏及偵測 HTML5 用戶端儲存中敏感資訊儲存情況相關的隱私權違規。

Dynamic Code Evaluation:Code Injection

研究資料表明，Pivotal 開發的 Spring Framework 易於遭受遠端程式碼執行弱點 (編號為 CVE-2018-1270) 的攻擊。此弱點可讓攻擊者透過 WebSocket 端點將惡意訊息傳送至暴露的 STOMP，這可能導致遠端程式碼執行。 本版本包含一項檢查，用於偵測 Spring Framework 中的這類弱點。該項檢查可透過 WebSocket 原則存取。

WebSocket Discovered

本版本包含一項資訊檢查，可指出在掃描的應用程式中是否存在 WebSocket。 此外，該項檢查會針對我們的客戶觸發提醒，讓其考慮使用包含與 WebSocket 弱點相關之所有檢查的新 WebSocket 原則來掃描應用程式。

合規報告

DISA STIG 4.8

為了在合規領域支援我們的聯盟客戶，本版本包含 WebInspect 檢查與最新版本 Defense Information Systems Agency Application Security and Development STIG 4.8 版之間的關聯性。

PCI DSS 3.2.1

本版本支援最新版本的 Payment Card Industry Data Security Standard (DSS) 合規範本 3.2.1 版。

原則更新

DISA STIG 4.8

在 WebInspect SecureBase 內現有的支援原則清單中，已新增為納入與 DISA STIG 4.8 相關的檢查而自訂的原則。

WebSocket

新 WebSocket 原則會對應用程式執行安全性評估，來判斷其是否有 WebSocket 相關弱點。

Micro Focus Fortify Premium Content

研究團隊在我們的核心安全情報產品之外建置、延伸並維護各種資源。

DISA STIG 4.8[2]

[2] 需要有 Fortify SSC 18.20 或更高版本，才能支援 DISA STIG 4.8 和 PCI DSS 3.2.1 報告。

為了呼應新的關聯性，本版本也包含支援 DISA STIG 4.8 的新 Fortify SSC 報告套件，您可以從 Fortify 客戶支援入口網站的 Premium Content 下方進行下載。

PCI DSS 3.2.1[1]

為了呼應新的關聯性，本版本也包含支援 PCI DSS 3.2.1 的新 Fortify SSC 報告套件，您可以從 Fortify 客戶支援入口網站的 Premium Content 下方進行下載。

Micro Focus Fortify Taxonomy:軟體安全性錯誤

Fortify Taxonomy 網站包含了新增類別支援的說明，其位址為：https://vulncat.fortify.com。 客戶若在舊網站尋找最新的支援更新，可從 Micro Focus Fortify 支援入口網站取得該更新內容。

連絡 Fortify 技術支援
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

連絡 SSR
Alexander M. Hoole
軟體安全性研究經理
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

2018 年 12 月 14 日