Micro Focus

Fortify 軟體安全性內容

2020 更新 2

2020 年 6 月 26 日

關於 Micro Focus Fortify Software Security Research

Fortify Software Security Research 團隊將尖端研究成果轉變為可為 Fortify 產品組合 (包括 Fortify Static Code Analyzer (SCA)、Fortify WebInspect 和 Fortify Application Defender) 增添動能的安全情報。現在，Micro Focus Fortify 軟體安全性內容能夠跨 27 種程式設計語言支援 1,022 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 Software Security Research (SSR) 欣然宣布，現已推出以下產品的更新：Fortify Secure Coding Rulepacks (英文，2020.2.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)，以及 Fortify Premium Content。

Micro Focus Fortify Secure Coding Rulepacks [SCA]

隨著此發佈，Fortify Secure Coding Rulepacks 能夠跨 27 種程式設計語言偵測 810 種獨特的弱點類別，且涵蓋 100 多萬個單獨 API。概括地說，此發佈包含下列項目：

Kotlin 核心程式庫支援 (1.3 版)[1]

對 Kotlin 標準程式庫的初始支援，涵蓋以下針對 JVM 的套件：

- kotlin
- kotlin.collections
- kotlin.comparisons
- kotlin.io
- kotlin.properties
- kotlin.random
- kotlin.ranges
- kotlin.sequences
- kotlin.streams
- kotlin.text

有限的 Java 互通性意味著 Java 支援的所有類別和程式庫在 Kotlin 中都是局部支援，以及專門針對 Kotlin 標準程式庫支援以下項目：

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial of Service: 規則運算式
- Denial of Service: StringBuilder
- Formula Injection
- Insecure SSL: Overly Broad Certificate Trust
- 記錄檔偽造
- Path Manipulation
- Poor Logging Practice: Use of a System Output Stream
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak
- System Information Leak: External
- System Information Leak: Internal
- 信任邊界違規
- Unchecked Return Value

[1] 需要 SCA 20.1.2 修補程式版本。使用 SCA 20.1 將會導致多個有關規則和特定 lambda 函數的錯誤，安裝此修補程式版本後，這些錯誤就不會發生。

C# 8 和 .NET 核心改進功能

已更新對 C# 8 和 .NET 核心程式庫 (包括 2.1、2.2、3.0 和 3.1 版) 的支援。藉此提供對 .NET Standard 2.1 的完整規則支援，還有改善使用 C# 8 非同步 *foreach*、*range* 和 *using* 運算時的資料流程。

Python 核心程式庫改進功能[2]

已更新對 Python 核心程式庫 (包括 3.7 和 3.8 版) 的支援。除了以前支援的類別之外，現在更進一步支援以下新類別：

- Python Bad Practices: Leftover Debug Code

Go 核心程式庫支援改進功能 (1.13 版)

擴大對 Go 核心程式庫的支援以涵蓋 crypto/tls。Go 是 Google™ 設計的靜態型別開放原始碼語言，旨在協助輕鬆建構簡單、可靠且高效率的軟體。Go 在語法上與 C 相似，但具有記憶體安全機制、垃圾回收及結構型別。支援的類別包括：

- Insecure SSL: Server Identity Verification Disabled
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- System Information Leak: External

GORM (1.9.12 版)

支援 GORM 程式庫，這是使用 Jinzhu 為 Golang 編寫的開放原始碼物件關係對應 (ORM) 專案。GORM 是一種常見的 ORM 程式庫，可能對企業應用程式帶來資料庫相關風險。支援的類別包括：

- Access Control: Database
- Connection String Parameter Pollution
- Dynamic Code Evaluation: Code Injection
- Insecure Transport
- 記錄檔偽造
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak: Internal
- Weak Cryptographic Hash

[2] 需要使用 SCA 20.2，才能在專案包含新引進的語法 (例如指派運算式) 時獲得更好的結果。

OWASP ASVS 4.0

為支援尋求框架以協助執行 appsec 程式的客戶，此版本支援 Micro Focus Fortify Taxonomy 類別與 OWASP Application Security Verification Standard 4.0 版需求之間的關聯性。ASVS 提供需求 (或測試) 清單，客戶可以使用它們來協助定義、建立和測試應用程式，並驗證應用程式是否安全。

其他勘誤

在此發佈中，我們持續盡可能投入一切資源，來確保我們可以降低誤報問題數，並提升客戶稽核問題的能力。客戶還會看到與下列各項相關回報問題的變更：

領域變更：

在某些特定地方，為保持一致性，已變更特定類別的領域。在較舊版本的 SCA (版本低於 6.30，亦即 2015-04-17 之前的任何版本) 中，這可能會導致某些問題在合併時被視為新增/已移除狀態，而不是保持為「已更新」狀態。SCA 6.30 或以上的所有版本不會發生此問題。
如果使用者依領域進行篩選，這通常也會影響篩選功能。受影響的類別包括：

- Access Control: ACL Manipulation。已從 "Input Validation and Representation" 變更為 "Security Features"
- Access Control: Authorization Bypass。已從 "Input Validation and Representation" 變更為 "Security Features"
- System Information Leak: Struts 2。已從 "Input Validation and Representation" 變更為 "Encapsulation"

誤報改進功能：

我們持續傾聽客戶的意見，致力於改善誤報率。在此版本中，我們完成以下工作，以減少誤報次數：

- 已移除導致多個類別誤報的特定 JavaScript 來源規則。
- Java "Unreleased Resource: Database" 規則已經過改進，可根據 JDBC 4.3 規格處理關閉基礎資源的連線問題。
- 已移除 Java 中關於 File.createTempFile() 誤報的 "Path Manipulation" 問題。
- 已停用從 TypeScript 定義檔案回報問題。
- 已在 SendAsync 上移除某些 .NET "Server-Side Request Forgery" 誤報。
- 已減少 Java "Spring Security Misconfiguration: Incorrect Request Matcher Type" 誤報。
- 已移除重複的 .NET "Weak Encryption" 問題。
- 已在 String 類型上移除 .NET "ASP.NET Bad Practices: Non-Serializable Object Stored in Session" 誤報。
- 已移除因 net.http.Response 物件意外感染而導致的 Golang 誤報。
- 已識別並移除 Java 中罕見的 "Code Correctness: Class Does Not Implement equals" 誤報。
- 在 JavaScript 中，已移除許多誤報的 "Key Management" 問題，並且在後續的版本中將繼續進一步改善。

錯誤和警告：
使用 SCA 19.2 時，對於任何支援的程式設計語言來說，若與整套 2020.2.0 Rulepack 結合使用，在掃描期間載入規則將會導致在建立和掃描記錄中產生以下警告：

```
[WARN  20599]
The rule language kotlin has no corresponding mapping in SCA
```

這是 SCA 19.2 的已知問題，可以透過移除以下 Kotlin Rulepack 檔案來解決：
<FORTIFY_DIR>\Fortify_SCA_and_Apps_19.2.0\Core\config\rules\core_kotlin.bin
掃描 Kotlin 需要使用 SCA 20.1.2。

VulnCat 改進功能
我們改進了篩選器類別及篩選器子類別的排序方式，讓項目以邏輯順序顯示。

ESAPI 驗證支援
我們聽取了客戶的意見，很多人對於 SCA 規則允許 ESAPI API 將問題移除做為修正方式感到擔憂，因為這是攸關程式庫的安全性疑慮。
從這個版本開始，我們從 ESAPI 程式庫中移除了驗證機制，現在資料流程將透過編碼功能繼續，而不會造成資料流程問題無法出現。
由於我們知道某些客戶希望繼續使用 ESAPI 程式庫 (特別是針對舊產品)，因此我們將提供再次納入此驗證的獨立 Rulepack。

如果您想繼續使用 ESAPI，可使用我們的 ESAPI 延伸模組 Rulepack (位於支援入口網站的 Premium Content, Fortify Exchange 下)。

請注意，此更新也會移除所有標記為 "Obsolete: Deprecated by ESAPI" 的問題，同樣地，您也可以使用上述的獨立 Rulepack 找到此更新。

Weak Encryption 更新
3DES 官方名稱為三重資料加密演算法 (Triple Data Encryption Algorithm，TDEA)，現在將根據美國國家標準與技術研究所 (NIST) 的建議在 Weak Encryption 下方進行回報。

Micro Focus Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 將數千個弱點的檢查，與在透過 SmartUpdate 立即取得的以下更新中引導使用者的原則結合在一起：

弱點支援

Web Server Misconfiguration: Information Disclosure

Spring Boot 包含許多其他功能 (也稱為傳動器)，可讓管理員監控和管理其網路應用程式。此版本包括了一項檢查功能，可偵測不具權限的使用者是否可使用敏感的 Spring Boot Actuator。攻擊者可以透過使用這類傳動器端點，收集稽核、健全狀況和度量資訊，甚至可以對某些配置執行「遠端程式碼執行」攻擊。

Cross-Site Scripting: Reflected

ASP.NET API ResolveUrl 用於解析執行階段時的應用程式根目錄相對路徑。此 API 無法驗證包括無 Cookie 狀態 ID 格式值的相對路徑，所以攻擊者能對應用程式進行 Cross-Site Scripting 攻擊。此版本包括了一項檢查功能，可用於偵測 .NET 應用程式中是否有此弱點。

Cookie Security: Missing SameSite Attribute

Cookie 上的 SameSite 屬性提供一種簡單的機制來保護應用程式避免 Cross-Site Request Forgery 攻擊。最新的瀏覽器版本可能會拒絕未設定 SameSite 屬性的 Cookie。此版本包括了一項檢查功能，可用於偵測設定的 Cookie 執行個體是否未設定 SameSite 屬性。

Cookie Security: Misconfigured Prefix

名稱開頭為 _Host- 或_Secure- 的 Cookie 會強制執行主機層級限制，且該 Cookie 只能透過安全的 HTTPS 連線傳送，以防止意外遭受竊聽和詐騙攻擊。瀏覽器可能會拒絕未適度設定 Path、Domain 和 Secure 屬性的 Cookie。此版本包括了一項檢查功能，可用於偵測字首配置錯誤的 Cookie。

Cookie Security: Overly Permissive SameSite Attribute

Cookie 上 SameSite 屬性的 Strict 值會強制瀏覽器僅將該 Cookie 附加至由於頂層導覽至網域或同一主機從含有連結 (例如 iframe、link 和 form 等) 的各種 HTML 標記發出要求而導致的要求。階段作業 ID 應使用 SameSite 屬性的 Strict 值設定，以為應用程式提供最大保護，使其避免 Cross-Site Request Forgery 攻擊。此版本包括了一項檢查功能，可用於在階段作業 Cookie 的 SameSite 屬性未設定為 Strict 時偵測執行個體。

合規報告

OWASP Application Security Verification Standard (ASVS)

OWASP ASVS 提供一種測試網路應用程式安全性控制的方法，還提供安全的開發準則。此版本包含將 WebInspect 檢查關聯至 OWASP ASVS 4.0 最新版本的功能。

原則更新

OWASP Application Security Verification Standard (ASVS) Policy

除了將 WebInspect 檢查關聯至 OWASP ASVS 最新版本之外，此版本還包括一項原則，可用於識別導致與 OWASP ASVS 相關聯的弱點。

其他勘誤：

在此發佈中，我們持續盡可能投入一切資源，來確保我們可以降低誤報問題數，並提升客戶稽核問題的能力。客戶還會看到與下列各項相關回報問題的變更：

- 針對 Often Misused: Weak SSL Certificate 對安全性內容進行改善後，現在可以更準確反映憑證為何被視為弱憑證的資訊。新增了 ID 為 11635 的新檢查功能。

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。

OWASP Application Security Verification Standard (ASVS)：

Application Security Verification Standard (ASVS) 是軟體開發週期 (SDLC) 期間執行的應用程式安全要求和測試清單，以及用來建立安全軟體的組態。隨著我們與產業合作夥伴協同合作改進對應的設計方式，我們預期此對應將會繼續演進。為了呼應新的關聯性，本版本也包含支援 OWASP ASVS 4.0 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，網址為：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

2020 年 6 月 26 日