Micro Focus

Fortify 軟體安全性內容

2020 更新 1

2020 年 3 月 27 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 26 種程式設計語言支援 1,019 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，2020.1.0 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 26 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：

GoLang 標準程式庫支援 [1]

擴大對 Go 標準程式庫的支援。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。此更新涵蓋標準程式庫命名空間，並支援 53 種弱點類型，包括下列 19 種額外類別：

- Denial of Service: 規則運算式
- Formula Injection
- Insecure Randomness
- JSON 注入
- 金鑰管理：空白 HMAC 金鑰
- 金鑰管理：硬式編碼的 HMAC 金鑰
- 記錄檔偽造
- 記錄檔偽造 (偵錯)
- Resource Injection
- Weak Cryptographic Hash
- 弱式密碼編譯雜湊：硬式編碼的 Salt
- 弱式密碼編譯雜湊：使用者控制的 Salt
- 弱式密碼編譯簽章：金鑰大小不足
- 弱式密碼編譯簽章：使用者控制的金鑰大小
- 弱式加密：RSA Padding 不足
- 弱式加密：不安全的初始化媒介
- 弱式加密：資料流加密
- 弱式加密：使用者控制的金鑰大小
- XML 注入

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：

- 在 JavaScript 中，更精確地識別為 self-XSS 的 "Cross-Site Scripting: DOM" 執行個體已變更為新的子類別 "Cross-Site Scripting: Self"，而且現在標示為較低優先順序。
- 在 Java 中，因為建模引擎的改進，Dead Code 誤判的數量無意間增加了，特別是關於 if- 條件。規則已獲得改善，因此不再有許多無效問題。

[1] 建議使用 SCA v20.1.0 或更新版本以獲得最佳掃描結果。

- 與 JSP 和 Spring MVC 應用程式有關的罕見效能問題已經解決。
- 更新了外部中繼資料以改善與 Micro Focus Fortify 的 Common Weakness Enumeration (CWE™) 關聯性：軟體安全性錯誤分類法 (也稱為 7 Pernicious Kingdoms)。這些改善包括在軟體安全性錯誤分類法的 935 個類別中調整了 41 個額外 CWE-ID，因此更新了 CWE 和 CWE Top 25 2019 對應關係。CWE 的任何相關報告功能或「分組依據」篩選器必然會受到影響。額外的 CWE ID 包括下列項目：

  CWE-88、CWE-97、CWE-119、CWE-147、CWE-192、CWE-203、CWE-212、CWE-266、CWE-267、CWE-276、CWE-279、CWE-280、CWE-346、CWE-347、CWE-436、CWE-506、CWE-527、CWE-529、CWE-530、CWE-531、CWE-536、CWE-540、CWE-541、CWE-548、CWE-550、CWE-705、CWE-775、CWE-799、CWE-917、CWE-921、CWE-923、CWE-925、CWE-926、CWE-937、CWE-942、CWE-1004、CWE-1021、CWE-1069、CWE-1173、CWE-1188、CWE-1236、

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

危險的檔案包括：本機

嚴重影響 Tomcat 的漏洞會利用 AJP 通訊協定功能來取得對伺服器端檔案的存取權，並允許攻擊者讀取或包含 Apache Tomcat webapp 目錄中的任何檔案。此弱點稱為 GhostCat，由 CVE-2020-1938 識別。此外，也可能發生任意程式碼執行攻擊。此問題會影響 Apache Tomcat 9.x (9.0.31 之前)、8.x (8.5.51 之前)、7.x (7.0.100 之前)，以及所有較舊版本。此 Securebase 更新包含可用來偵測此弱點的檢查。

Common Weakness Enumeration (CWE™) 對應關係：

Common Weakness Enumeration (CWE™) 是一種軟體錯誤分類法，這些軟體錯誤可能導致軟體弱點。該分類法提供一種方法，可在 SDLC 各個階段合併軟體風險和弱點評估中各種方法的輸出。在此版本中，Securebase 包括 CWE 中最新更新檢查的已更新對應關係。CWE 是一種階層分類法。檢查會對應到符合檢查目的的最近分葉節點。

合規報告

Common Weakness Enumeration (CWE™) Top 25：

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Errors (CWE Top 25) 是由 MITRE 建立的清單。此清單展示可能了導致軟體弱點的 25 個最常見軟體弱點類別。此 Securebase 更新包含與這些 CWE 類別的對應關係。我們已包括那些直接對應到 CWE Top 25 所識別類別的檢查，或是透過 “ChildOf” 關係對應到 Top 25 中 CWE-ID 相關的 CWE-ID。

原則更新

Common Weakness Enumeration (CWE™)

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Errors (CWE Top 25) 是由 MITRE 建立的清單。此清單展示了可能導致軟體弱點的 25 個最常見軟體弱點類別。此版本包含一個原則，其中含有用來評估與 CWE Top 25 中對應的弱點的檢查清單。

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：

- HTTP Request Smuggling 檢查中的錯誤修正包括減少了與使用檢查 ID 11621 尋找有關的誤判。此檢查不會再將 HTTP 405 視為該弱點的有效驗證。
- 不安全的傳輸：弱式 SSL 加密報告內容現在包括一個範例，該範例透過在組態字串中包含 !SHA246 和 !SHA384 來排除 CBC 模式加密。但是，我們建議您諮詢伺服器管理員，使用加入白名單的強式加密套件選項來建立組態。
- Insecure Transport 中的額外修正：如果伺服器僅支援 TLS1.2 和強式加密，則在檢查無法偵測到正確加密的情況下，會進行弱式 SSL 加密偵測以改善配置偵測。

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。我們已經建立 Securebase 檢查和 SCA 規則對該標準適用要求的對應關係。但是，在建立與我們產品的關聯性的過程中，我們發現一些項目，其中可以改善標準所提供的 CWE 對應關係，以更準確地與 Securebase 檢查和 SCA 規則保持一致。在進行這些改善時，我們可將這些成品提供給感興趣的客戶進行評估和協作。如果您有興趣，請連絡以下的 SSR 連絡人，以取得 WebInspect 或 SSC 種子套件的合規性範本和原則。

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 3 月 27 日