Micro Focus

Fortify 軟體安全性內容

2021 更新 1

2021 年 3 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 1,038 個弱點類別，且涵蓋 100 多萬個單獨 API。

瞭解詳情：https://software.microfocus.com/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，2021.1.0 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 27 種程式設計語言偵測 816 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：

Micro Focus Visual COBOL 支援 (第 6 版)[1]

此發佈新增對 Micro Focus Visual COBOL 第 6 版的支援。尤其是此發佈包括對 Micro Focus COBOL 執行階段系統 (RTS) 的支援，並擴充對 COBOL 早已支援的 Path Manipulation 類別和以下其他類別的支援：

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

Android 11

我們持續致力於支援 Android 最新版本 (API 版本 30)，納入了以下命名空間：

- android.accounts
- android.app
- android.database
- android.database.sqlite

使用者應該會看到更好的 Android 應用程式建模，這些建模通常可以改善結果，以及其他 *SQL Injection* 和 *Access Control: Database* 發現項目。

iOS 更新

我們持續致力於改進 iOS 支援，針對以下類別新增 Swift 規則：

- Foundation.NSCache
- Foundation.URLFileProtection

使用者應該會看到與 Data Protection 和 Privacy Violation 有關的改善結果，以及其他弱點類型和框架的一般改進功能 (請參閱「其他勘誤 - iOS 錯誤修正」)。

Angular 支援更新 (11.2.3 版)

此發佈將我們的 Angular 支援提升至 11.2.3。尤其是，識別出瀏覽器中使用者控制資訊的新來源，這可能導致許多類別在過去未曾觸發過的位置觸發。

[1] 需要 SCA 21.1 或更新版本。

Apache Commons 更新

Apache Commons 提供可重複使用的 Java 元件。在此發佈中，SSR 更新了以下元件的支援：

- beanutils (1.9.4)
- collections4 (4.4)
- dbutils (1.7)
- fileupload (1.4)
- lang (3.11)
- math (3.6.1)
- io (2.8.0)
- text (1.9)

這些更新可改進使用這些元件的應用程式的建模，識別出防止 Log Forging 和 JSON Injection 等類別的保護措施，同時也識別出可能出現以下弱點類型的新位置：

- Access Control: Database
- Denial of Service
- Insecure Randomness: User-Controlled Seed
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak (變體)

Python (3.9 版)

已更新對 Python 最新版本的支援，從而改進核心語言 API 的建模。

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：

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：

- *Code Correctness: Erroneous Class Compare* (在 Java 和 Kotlin 應用程式中)
- *Dynamic Code Evaluation: Code Injection* 問題已於 Python 3 掃描作業中移除
- *Key Management* 問題已獲得改善，進而移除所有語言中的誤報問題
- *Cross-Site Scripting: DOM* 問題 (與 jQuery 有關) 來自輸入方塊時，現已正確分類為 *Cross-Site Scripting: Self*。
- 已移除在比對不能為密碼的內容時組態檔中的 *Password Management* 問題
- 改進了比對當地語系化資料時 *Password Management* 的誤報。
- 已在 Java Spring 應用程式中不相關功能上移除 *XML External Entity Injections* 發現項目。
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* 現在允許將其他動詞視為安全 (PATCH、DELETE、PUT)。

iOS 錯誤修正：
由於分析功能的改善，所以也需要更新規則。這進而可讓使用者看到以下弱點類型的改善：
- Input Interception: Keyboard Extensions Allowed
- Privacy Violation: HTTP Get
- Privacy Violation: Keyboard Caching
- Privacy Violation: Screen Caching
- Privacy Violation: Shoulder Surfing

幾個框架也已完成小幅度的更新，以提高準確性：Foundation、UIKit、WebKit、HealthKit、WatchKit、MessageUI、CoreLocation、CoreData。

已移除的類別：
為增強結果的相關性，此發佈已移除以下類別：
- Privilege Management: Android Network

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

OGNL Expression Injection: Struts 2

CVE-2019-0231 和 CVE-2020-17530 所識別出的重大 OGNL Expression Language injection 漏洞會影響 Struts 2.0 至 2.5.25 版。利用這些漏洞可能導致在伺服器上執行任意遠端程式碼。此發佈包括了一項檢查功能，可用於偵測使用 Struts 2 的 Web 應用程式中是否有這些弱點。

WAF Detection[2]

此發佈包括了「WAF Detection」檢查功能，可在掃描過程中偵測到 Web 應用程式防火牆時，標記資訊發現項目。這些發現項目表示，由於掃描要求在到達應用程式之前即被封鎖，因此掃描品質可能會受到影響。

Hacker Level Insights[2]

Hacker Level Insights 可為開發人員和資訊安全專業人員提供與應用程式整體安全性狀況有關的內容。此發佈包括了一項檢查功能，可標記掃描過程中在應用程式中偵測到的程式庫。儘管這些發現項目不一定代表安全性漏洞，但務必注意攻擊者通常會對這些類型的目標執行偵察，試圖找出已知的弱點或模式。

[2] 需要 WebInspect 21.1 或更新版本。

原則更新

NIST SP 800-53 修訂版 5

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 NIST SP 800-53 修訂版 5 相關的檢查而自訂的原則。

CWE Top 25 2020

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 CWE Top 25 2020 相關的檢查而自訂的原則。

DISA STIG 5.1

在 WebInspect SecureBase 支援的原則清單中，已新增為納入與 DISA STIG 5.1 相關的檢查而自訂的原則。

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：

Web Cache Poisoning
此發佈包括一項更新的檢查功能，適用於 *Web Cache Poisoning: Unkeyed Headers*。使用者現在可以新增他們懷疑是 cache-key 一部分的自訂標頭。

不安全的 SpringBoot Actuator
此發佈包括一項更新的檢查功能，可偵測不具權限的使用者是否可使用敏感的 Spring Boot Actuator，這項更新的檢查功能提供更準確的結果。

XSS 改進功能
此發佈包括改進的 XSS 攻擊檢查功能，適用於 Vue 3 和 Angular JS 1.5.9 及以上版本。

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。

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

2021 年 3 月 26 日