Micro Focus

Fortify 軟體安全性內容

2019 更新 1

2019 年 3 月 29 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 999 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) 很高興地宣佈，現已推出以下產品的更新：Fortify Secure Coding Rulepacks (英文，2019.1.0 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 796 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：

Angular 7[1]

支援 Angular (包括對最高 7.0.0 版 (含) 的支援) 可識別瀏覽器的輸入來源，並為預設由 Angular 執行的安全驗證建立模型。系統會為 Angular 範本建立模型，以使 Angular 專案支援所有的一般 JavaScript 接收器，其中包括能夠尋找類別，例如 Cross-Site Scripting:DOM、Privacy Violation、Dynamic Code Evaluation 等問題。

AWS Lambda 函數支援

新增對 Java 和 Python 語言的 Amazon Web Services (AWS) Lambda 函數支援。功能可實現從 Lambda 觸發事件到 Lambda 函數邏輯的資料流，包括涵蓋 Lambda 連線至 API 閘道時的潛在 XSS 問題。

AWS Java SDK v2

針對 S3 和 DynamoDB 服務新增對 AWS Java SDK v2 的支援。包括新類別，例如：

- Access Control: ACL Manipulation
- Insecure Storage:S3 Full Anonymous Access
- Insecure Storage:S3 Read ACP Anonymous Access
- Insecure Storage:S3 Read Anonymous Access
- Insecure Storage:S3 Write Anonymous Access
- Insecure Storage:S3 Write ACP Anonymous Access
- NoSQL Injection:DynamoDB

Python Django[1]

更新對 Python Django Web Framework 的支援，包括對最高 2.1.7 版的支援。變更事項包括改善對類別型檢視和相關資料流的支援，還有支援自 Django 1.8 開始引入的 Django 函數/方法。

Apache Wicket[1]

改善對 Apache Wicket Web Framework 的支援，包括對第 6、7 和 8 版架構的支援。

DISA STIG 4.9

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 4.9 版之間的關聯性。

[1] 若要支援 Angular 7、Django 和 Wicket，將需要 Fortify SCA 19.1.0 或更新版本以獲得最佳效果。

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

常遭不當使用的功能：檔案上傳

經判定，Blueimp 的 jQuery File Upload 小工具易遭受遠端程式碼執行弱點 (識別碼為 CVE-2018-9206) 的攻擊。此弱點可讓攻擊者上傳並執行任意 PHP 檔案。本版本包含一項檢查，可用來偵測此弱點。

SQL Injection

本版本包含 SQL Injection 檢查的增強功能，以納入對使用 Microsoft Azure SQL 資料庫的應用程式的支援。

敏感資訊洩漏：外部

本版本包含一項檢查，可用來偵測 Magento CMS 是否以開發人員模式執行。開發人員模式主要用於開發或測試環境。在生產環境中啟用開發人員模式可能將重要的應用程式和系統資料洩漏給潛在攻擊者，並引致安全性風險。

跨框架指令碼

內容安全性原則 *frame-ancestors* 指令標頭提供針對跨框架指令碼弱點的原則保護。它會使目前使用中的 X-Frame-Options HTTP 標頭過時。 本版本包含現有跨框架指令碼檢查的增強功能，以納入對內容安全性原則 frame-ancestors 指令的支援。

內容管理系統 (CMS) 指紋

本版本包含在 WebInspect 掃描期間，辨別目標伺服器上是否存在下列其中一個 CMS 的增強功能：WordPress、Drupal、Django、Joomla、Liferay、Magento、Sitecore、Sitefinity[2] 及 Umbraco。系統會觸發資訊檢查來回報此發現。

合規報告

DISA STIG 4.9

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 4.9 版之間的關聯性。

[2] 若要使用 Sitefinity 偵測功能，將需要 WebInspect 19.1.0 或更新版本。

原則更新

DISA STIG 4.9

在 WebInspect SecureBase 內現有的支援原則清單中，已新增為納入與 DISA STIG 4.9 相關的檢查而自訂的原則。

Micro Focus Fortify Application Defender

Fortify Application Defender 是一款執行階段應用程式自我保護 (RASP) 解決方案，可協助組織透過自主開發或第三方應用程式來管理和降低風險。它可以集中查看應用程式使用和濫用情況，還可即時防範對軟體弱點的利用和其他違規現象。針對此版本，Micro Focus Fortify 軟體安全性研究團隊提供了以下改進功能：

OGNL Expression Injection：Struts 2

擴大對 Apache Struts 2 中 OGNL Expression Injection 偵測的支援，其中涵蓋識別碼為 CVE-2018-11776 的重大 Struts 弱點。如果使用 Apache Struts2 2.3.x 至 2.3.34 版或 2.5.x 至 2.5.16 版本的應用程式，所包含的動作結果未設定有命名空間或萬用字元命名空間，還在 struts 組態中將 struts.mapper.alwaysSelectFullNamespace 屬性設為 true，則會允許攻擊者執行任意 OGNL 運算式。

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 4.9[3]

為了呼應新的關聯性，本版本也包含支援 DISA STIG 4.9 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。

[3] 支援 DISA STIG 4.9 報告需要 Fortify SSC 18.20 版或更新版本。

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

2019 年 3 月 29 日