Micro Focus

Fortify 軟體安全性內容

2019 更新 2

2019 年 6 月 28 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 1,005 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，2019.2.0 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 799 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：

.NET 更新

支援 .NET Framework 4.7.1 版和 4.7.2 版中引入的 API 新增項。更新包括對 .NET Standard 2.0 和 .NET Core 2.0 的規則支援，其中涵蓋與 .NET Framework 相同的類別。更新的 .NET Framework 版之規則包括對下列類別的增強型支援：

- Header Manipulation:Cookies
- Insecure SSL:Server Identity Verification Disabled
- Insecure Transport:Weak SSL Protocol
- Weak Cryptographic Hash
- Weak Cryptographic Signature:Insufficient Key Size
- Weak Encryption

Realm 資料庫

Realm 資料庫是一個開放原始碼輕量型資料庫，專門為行動應用程式而設計，現在支援 iOS (Swift 和 Objective-C) 以及 Android (Java)。支援的類別包含以下幾類：

- Access Control:Database
- Key Management:Empty Encryption Key
- Key Management:Hardcoded Encryption Key
- Key Management:Null Encryption Key
- Path Manipulation

此外，還支援兩個新類別：

- Insecure Storage:Missing Database Encryption
- NoSQL Injection:Realm

Python urllib3

現在支援 Python urllib3 程式庫 (一個功能強大的常用 HTTP 用戶端)。類別涵蓋範圍包括以下幾類：

- Header Manipulation
- Insecure SSL:Server Identity Verification Disabled
- Password Management
- Password Management:Empty Password
- Password Management:Hardcoded Password
- Password Management:Null Password
- Password Management:Weak Cryptography
- Server-Side Request Forgery

Java SE 10 和 11 更新

Java SE 的涵蓋範圍現在已擴充至版本 10 和 11，包括對新 HTTP 用戶端 API 的支援。

Cross-Site Scripting:SOP Bypass

JavaScript 和 TypeScript 內對於新類別 "Cross-Site Scripting:SOP Bypass" 的支援。這個新類別涵蓋特別情況，即攻擊者會利用弱點來避開相同原始原則 (SOP)，藉此發動 Cross-Site Scripting 攻擊。

PCI SSF 1.0

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 Micro Focus Fortify Taxonomy 類別與新的「安全軟體需求與評估程序」(在支付卡產業 (PCI) 安全軟體標準 (SSS) 中定義，作為新的軟體安全性架構 (SSF) 1.0 版的一部分) 中所指定控制目標之間的關聯性。新標準最終會取代 PCI 資料安全標準 (DSS)，取而代之的是新的支付應用程式 (PA) DSS (提交截止到 2020 年年中)，而現有 PA-DSS 的變更會在 2022 年到期。

其他勘誤

在本版本中，我們繼續盡可能善用一切資源，來確保降低誤報問題數，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的所回報問題的變更：

Log Forging

降低所有語言的誤報數，因為可以更準確地識別能夠移除新行的 API，藉此來防止發生 Log Forging 和 Log Forging (偵錯) 問題。

Unreleased Resource:Database

在 Java 內，如果建立結果集的陳述式先關閉，則演算法會無法正確識別該結果集是否自動關閉。相關的誤報現在已消除。

Unsafe JNI 和 Unsafe JSNI

升級至 SCA v19.1.x 的客戶在使用 Java 應用程式時可能會發現有新的 "Unsafe JNI" 和 "Unsafe JSNI" 問題大量出現。此種情況是由於引擎改進所造成。這意味著大量 API 標記客戶無法控制修復的情形。此問題現在已糾正，SCA 僅標記使用者可以控制來源的 API。隨著問題的減少，客戶亦可能注意到 "Access Control:SecurityManager Bypass" 問題的減少。

Dynamic Code Evaluation 和 Lambda 上的其他接收器

在 JavaScript 應用程式中，lambda 呼叫引起的問題可能會導致出現混淆結果。此種情況的常見範例是 setTimeout()。這些無關緊要的問題現已移除，儘管在某些情況下仍可能發生，但我們正在積極努力地降低其發生頻率。僅在使用 SCA v18.20 或更新版本時才會注意到此頻率已降低。

Cross-Site Scripting:Content Sniffing 支援

過去，當回應的 content-type 阻止瀏覽器處理 HTML/JS 內容 (例如，application/json) 時，SCA 會報告 Cross-Site Scripting 問題。原因是 Web 應用程式的使用者可能使用的是較舊的瀏覽器，而這些瀏覽器容易遭受內容探查攻擊。對於本版本，我們已修改這些問題，使其報告為 "Cross-Site Scripting:Content Sniffing"。這樣稽核者和開發人員便可快速識別這些問題，並將其與更嚴

重的 Cross-Site Scripting 情況區別開來。Java Rulepack 中的 Spring Framework 和 JAX-RS 均支援此新類別。

根據污點降低 Fortify 優先順序

過去，對於源自 HTTP 要求參數與源自系統環境變數的 SQL Injection，SCA 會報告相同的嚴重性。我們知道，攻擊者控制系統變數的可能性非常低，或至少低於控制要求參數的可能性。基於此，我們已降低某些情況中問題的 Fortify 優先順序值，但是，從本版本開始，SCA 將更一致地套用污點來源作為計算問題的 Fortify 優先順序值的新因素。

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

WebSocket 更新[1]

本版本包含多項增強功能，可偵測 WebSocket 流量中 Information Leak 和 Unsafe Deserialization (針對 .NET) 弱點。特別是已對下列類別進行增強，以支援 WebSocket：

- Dynamic Code Evaluation:Unsafe Deserialization
- Poor Error Handling:Unhandled Exception
- Privacy Violation
- Privacy Violation:Credit Card Number
- Privacy Violation:National ID Disclosure
- Privacy Violation:Social Security Number
- System Information Leak:Internal IP

安全回應標頭配置更新

伺服器會使用一組 HTTP 回應標頭，來提供可提高應用程式安全性的瀏覽器配置。這些標頭會視為深度防禦機制，可在經過設定後很好地防範弱點。本版本包含對下列標頭和相關類別的增強型支援：

- Cache-Control
  - Cache Management:Insecure Policy
- Content-Security-Policy
  - HTML5:Missing Content Security Policy
  - HTML5:Deprecated Content Security Policy
  - HTML5:Misconfigured Content Security Policy
- X-Content-Type-Options
  - Web Server Misconfiguration:Insecure Content-Type
- X-XSS-Protection
  - HTML5:Cross-Site Scripting Protection

[1]WebSocket 更新需要 WebInspect 19.1.0 或更新版本。

Web Server Misconfiguration:Deprecated SSL/TLS Certificate

Symantec 憑證授權單位 (包括 Symantec 所有的品牌，例如 Thawte、VeriSign、Equifax、GeoTrust 和 RapidSSL) 在 2017 年 12 月 1 日之前核發的所有 SSL/TLS 憑證均不再受信任，並且不再被 Chrome、Internet Explorer、Firefox 和 Safari 等所有主要瀏覽器接受。本版本包含的檢查可用於標記過時的 Symantec 憑證的使用。

Insecure Deployment:Unpatched Application

Drupal 內容管理系統 (CMS) 中識別為 CVE-2019-6340 的重大遠端程式碼執行弱點可讓遠端攻擊者在伺服器上執行任意程式碼。本版本包含的檢查可偵測部署了 Drupal CMS 的應用程式中是否有此弱點。

合規報告

PCI SSF 1.0

為了在合規領域支援我們的客戶，本版本包含新的合規範本，可將 Micro Focus Fortify Taxonomy 與新的「安全的軟體需求與評估程序」(在支付卡產業 (PCI) 安全的軟體標準 (SSS) 中定義，作為新的軟體安全性架構 (SSF) 1.0 版的一部分) 中所指定的控制目標相關聯。新標準最終會取代 PCI 資料安全標準 (DSS)，取而代之的是新的支付應用程式 (PA) DSS (提交截止到 2020 年年中)，而現有 PA-DSS 的變更會在 2022 年到期。

原則更新

PCI SSF 1.0

在 WebInspect SecureBase 內現有的支援原則清單中，已新增為納入與 PCI SSF 1.0 相關的檢查而自訂的原則。

其他勘誤

Cache Management:Insecure Policy

增強了檢查 ID 11306，以排除對特定 content-type 之 HTML 回應的標幟，這些 content-type 在手動驗證時通常會稽核為誤報結果。

Expression Language Injection:Spring

SecureBase 檢查 ID 11579 中弱點偵測演算法的準確性已得到提升。

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。

PCI SSF 1.0

為了呼應新的關聯性，本版本也包含支援 PCI SSF 1.0 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

2019 年 6 月 28 日