Micro Focus

Fortify 軟體安全性內容

2020 更新 4

2020 年 12 月 18 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 1,039 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，2020.4.0 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 817 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：

Dapper 支援 (2.0.78 版)

支援 Dapper 物件關係對應 (ORM)。Dapper 用於透過擴充 .NET IDdbConnection 介面，將原生查詢輸出對應到強型別 C# 物件。新支援會將 Dapper 視為使用者控制資料的來源，也會將其視為下列類別的觸發條件：

- Access Control: Database
- SQL Injection

Kotlin 標準程式庫更新 (1.3 版)

擴充對 Kotlin 標準程式庫的支援，以納入下列套件：

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull (第 1 版)

支援 Android 實作 XML Pull 套件。XML Pull 是一個簡單的串流 API，用於剖析和序列化 XML 檔案，檔案中的應用程式會控制剖析作業 (可中斷和繼續剖析作業)。支援的類別包括：

- XML Entity Expansion Injection
- XML 注入

AIOPG (1.0.0 版)[1]

支援 Python aiopg 程式庫。Aiopg 提供了一種非同步方式來連線至 PostgreSQL 資料庫。支援的類別包括：

- Access Control: Database
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- SQL Injection

[1] 完整偵測與 aiopg 相關的問題將取決於未來改進與「與...同步」相關的 SCA。

JavaScript Promises

- 針對資料流分析，已改進對 JavaScript Promises 的支援。

Azure 資源管理範本

初始支援 Azure 資源管理 (ARM) 範本。ARM 範本用於為 Azure 解決方案實作基礎架構即程式碼。ARM 範本是 JSON 檔案，會利用宣告式語法來定義和設定使用者的專案。支援的類別包括：

- Azure Resource Manager Misconfiguration: HTTPS Not Required
- Azure Resource Manager Misconfiguration: Public Access Allowed

DISA STIG 5.1

為了在合規領域支援我們的聯盟客戶，已新增 Micro Focus Fortify Taxonomy 與 Defense Information Systems Agency (DISA) Application Security and Development STIG 5.1 版之間的關聯性。

NIST SP 800-53 修訂版 5

為了在合規領域支援我們的聯盟客戶，我們新增了 Micro Focus Fortify Taxonomy 與最新版本美國國家標準與技術研究所 (NIST) Special Publication (SP) 800-53 修訂版 5 中安全性與隱私權控制之間的關聯性。內容涵蓋了三十個基礎控制，橫跨下列控制系列：

- Access Control (AC)
- 稽核與可歸責性 (AU)
- 評估、授權與監控 (CA)
- 組態管理 (CM)
- 識別與驗證 (IA)
- PII 處理與透明度 (PT)
- 系統與通訊保護 (SC)
- 系統與資訊完整性 (SI)

2020 Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE™) Top 25 於 2019 年推出，取代了 SANS Top 25。8 月發佈的 2020 CWE Top 25 是使用啟發式公式決定的，這個公式會將過去兩年回報給美國國家弱點資料庫 (National Vulnerability Database，NVD) 的弱點頻率及嚴重性正規化。為了支援我們的客戶，使其可以針對 NVD 中最常回報的重大弱點排列稽核作業的優先順序，已新增 Micro Focus Fortify Taxonomy 與 2020 CWE Top 25 之間的關聯性。

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：

不再支援 17.x 之前的 SCA 版本：
如我們 2020.3 發佈公告中所述，這是支援 17.x 之前的 SCA 版本的最後 Rulepack 版本。對於此本版本，17.x 之前的 SCA 版本將不會載入最新的 Rulepack。使用 17.x 之前的 SCA 版本的客戶必須降級 Rulepack 或升級 SCA 版本。

在未來的版本中，我們將會支援 SCA 的最後四個主要版本。

即將過時的對應
多年來，軟體安全性研究團隊一直持續建立從 Fortify 類別至外部標準和最佳實務的對應。因此，即使許多舊版本將不再使用，我們目前所支援之各種標準的版本數量也非常可觀。

所以，我們現在將下列標準標記為「已過時」：
- 支付卡產業資料安全標準 (PCI) 1.1
- 支付卡產業資料安全標準 (PCI) 1.2
- 支付卡產業資料安全標準 (PCI) 2.0
- 支付卡產業資料安全標準 (PCI) 3.0
- 支付卡產業資料安全標準 (PCI) 3.1
- 支付卡產業資料安全標準 (PCI) 3.2
- 安全性技術實作指南 (STIG) 4.1
- 安全性技術實作指南 (STIG) 4.2
- 安全性技術實作指南 (STIG) 4.3
- 安全性技術實作指南 (STIG) 4.4
- 安全性技術實作指南 (STIG) 4.5
- 安全性技術實作指南 (STIG) 4.6
- 安全性技術實作指南 (STIG) 4.7
- 安全性技術實作指南 (STIG) 4.8

這項變更意味著 Fortify SCA 應用程式 20.2 版和更高版本將預設為不顯示這些舊的對應。
如果您需要檢查是否符合這些舊版本，則必須變更對應，將 *obsolete* 屬性設為「false」，或完全移除該屬性。

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：
- 已移除當組態檔中存在保護時的 HTTP 動詞篡改誤報
- 已移除在 .NET 中使用 JSONIGNORE 屬性時的 Mass Assignment 誤報
- 已移除 URLSessionConfiguration 物件中明確停用快取時的 Insecure Storage: HTTP Response Cache Leak 誤報
- 已將 Swift Privacy Violation: Http Get 誤報從 URLRequest 中移除
- Poor Logging Practice: Use of a System Output Stream 重複部分已在 Python 中移除

- 已移除使用其他 Apache Commons closeQuietly 變體時的 Unreleased Resource 問題

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

弱式密碼編譯簽章：可預測的祕密金鑰

為了保護 JSON Web Token 承載的完整性，通常會使用 HMAC 簽章。但是，如果 HMAC 演算法使用弱式密碼，則惡意使用者將可透過暴力破解秘密金鑰，然後使用任何承載，對 JWT 進行重新簽署。此版本包括一項檢查，可用來識別是否使用常用密碼中的字串對 JWT 權杖進行簽署。

Password Management: Weak Password Policy

用於確保使用者建立強式密碼的密碼原則對部署安全的網站而言至關緊要。密碼應經過驗證，以確保它們不是常用密碼之一，且密碼字串應符合 NIST 800-53、NIST 800118 和 OWASP 設定的準則。此版本包括一項新檢查，可用來偵測登入巨集中設定的密碼是否與常用密碼之一相符。此版本也更新了弱式密碼原則檢查，以根據前述 NIST 標準和 OWASP 準則中的規定，滿足修訂的密碼強度準則。

Cache Management: Web Cache Poisoning

使用者首次造訪網站時，Web 快取會儲存網頁的副本。當使用者下次造訪同一網頁時，就會將快取的副本提供給使用者。但是，如果這些 Web 快取具有實作或設計漏洞，例如會接受具有要求本文的 GET 要求 (例如大量 GET 要求或未鍵入的輸入)，便可能受到 Web Cache Poisoning 攻擊。Web Cache Poisoning 是攻擊者用來為合法使用者快取惡意回應的一種先進技術。此版本包括一項檢查，可用來識別網站是否透過未鍵入標頭和大量 GET 要求可能受到 Web Cache Poisoning 攻擊。

合規報告

DISA STIG 5.1

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 5.1 版之間的關聯性。

NIST SP 800-53 修訂版 5

為了在合規領域支援我們的聯盟客戶，本版本包含 WebInspect 檢查與最新版本美國國家標準與技術研究所 (NIST) Special Publication (SP) 800-53 修訂版 5 中控制之間的關聯性。

2020 Common Weakness Enumeration (CWE™) Top 25

Common Weakness Enumeration (CWE™) Top 25 於 2019 年推出，取代了 SANS Top 25。8 月發佈的 2020 CWE Top 25 是使用啟發式公式決定的，這個公式會將過去兩年回報給美國國家弱點資料庫 (National Vulnerability Database，NVD) 的弱點頻率及嚴重性正規化。此 Securebase 更新包含與這些 CWE 類別的對應關係。我們納入了直接對應到 CWE Top 25 所識別的類別的檢查，或是透過「ChildOf」關係對應到 Top 25 中 CWE-ID 相關的 CWE-ID。

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：

- 已重新設計 HTTP Request Smuggling 檢查，以減少誤報、提高效率並提升其結果的準確性。檢查 ID 11621 不再使用時基法進行弱點驗證。

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 5.1、NIST SP 800-53 修訂版 5 和 2020 CWE Top 25

為了呼應新的關聯性，此版本也包含支援 DISA STIG 5.1、NIST SP 800-53 修訂版 5 和 2020 CWE Top 25 且適用於 Fortify Software Security Center 的新報告套件，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 12 月 18 日