Micro Focus

Fortify 軟體安全性內容

2019 更新 4

2019 年 12 月 13 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 1,018 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) 很高興地宣布，現已推出以下產品的更新：Fortify Secure Coding Rulepacks (英文，2019.4.0 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 26 種程式設計語言偵測 807 種獨特的弱點類別，且涵蓋 100 多萬個單獨 API。總而言之，此發佈包含下列項目：

Go 初始支援[1]

針對 Go 的初始支援。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 10 個核心標準程式庫命名空間，並支援以下 34 種類別：

- Access Control:Database
- Command Injection
- Connection String Parameter Pollution
- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cross-Site Scripting:Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting:Reflected
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: MIME Sniffing
- Insecure Transport
- Key Management:Empty Encryption Key
- Key Management:Hardcoded Encryption Key
- Key Management:Null Encryption Key
- Open Redirect
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Path Manipulation
- Path Manipulation:Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- SQL Injection
- System Information Leak: External
- System Information Leak:Internal
- Weak Encryption
- Weak Encryption:Insufficient Key Size

[1] 需要 SCA v19.2.0 或更新版本。

Spring Security

Spring Security 是一種驗證和存取控制架構，這個架構也能提供額外的安全層 (例如安全性標頭)，藉此提供阻擋工作階段固定、點擊劫持及跨網站請求偽造等攻擊的額外防護。這是保護以 Spring 為基礎的應用程式的業界標準。此更新支援以下 21 種類別 (最高 5.2.1 版)：

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: Overly Broad Domain
- Cross-Site Request Forgery
- Header Manipulation
- HTML5:Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Missing Content Security Policy
- HTML5:Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5:Overly Permissive Referrer-Policy
- Insecure Transport:HSTS Does Not Include Subdomains
- Insecure Transport:HSTS not Set
- Insecure Transport:Insufficient HSTS Expiration Time
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- Session Fixation
- System Information Leak

此外，還引入了以下七種新弱點類別：

- HTML5: Missing Framing Protection
- HTML5: Unenforced Content Security Policy
- Spring Security Misconfiguration: Default Permit
- Spring Security Misconfiguration: Disabled Security Headers
- Spring Security Misconfiguration: Incorrect Request Matcher Type
- Spring Security Misconfiguration: Lack of Fallback Check
- Spring Security Misconfiguration: Overly Permissive Firewall Policy

Spring Boot

Spring Boot 可建立獨立 Spring 應用程式，並盡可能自動配置 Spring 和第三方程式庫。另外，也會提供指標、健全狀況檢查及外部化配置等生產就緒功能。除了之前支援的類別，此更新還支援以下九種類別 (最高 2.2.1 版)：

- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Overly Broad Session Cookie Domain
- Cookie Security: Overly Broad Session Cookie Path
- Cookie Security: Persistent Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Password Management: Empty Password in Configuration File
- Insecure Transport
- Insecure Transport: Server Identity Verification Disabled
- System Information Leak:External

此外，由於之前的 Rulepacks 僅支援 Properties 配置檔和 Maven build 系統，所以此版本也支援 YAML 配置檔和 Gradle。

Java 12[2]

支援 Java 12 中的新 API。使用新的 Java 12 語法 (例如新的 Switch 陳述式) 時，這些規則需要 SCA 19.1 版或更新版本。

JSTL XML 程式庫

JavaServer Pages (JSP) Standard Tag Library (JSTL) 是一個程式庫，提供以 JSP 為中心的方式來操作及建立 XML 文件。現在對 JSTL v1.1 的支援涵蓋以下類別：

- XSLT Injection
- XML External Entity Injection
- Privacy Violation
- System Information Leak: External

OpenXML SDK .NET 改進

更新的 OpenXML SDK v2.9.0 支援包括對以下三種額外類別的支援：

- Access Control: Database
- Connection String Parameter Pollution
- SQL Injection

React-Router 支援

React Router 是一個導覽元件集合，這些元件透過您的應用程式以宣告方式撰寫。不論您是想為 Web 應用程式建立可加入書籤的 URL，還是在 React 中使用可組合的導覽方式，React Router 都能在 React 轉譯的位置發揮效用。React-Router 5.1.2 的支援類別包括：

- Open Redirect
- Privacy Violation
- System Information Leak: External

2019 CWE Top 25

Common Weakness Enumeration (CWE) Top 25 已徹底改變其過去稱為 SANS Top 25 時所用的報告決定方式。9 月發佈的新 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 CWE Top 25 2019 版之間的關聯性。

DISA STIG 4.10

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 4.10 版之間的關聯性。

[2] 需要 SCA v19.2.0 或更新版本。

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回報問題的變更：

- 不安全的還原序列化一致性：過去，有些規則只會標記資訊是來自瀏覽器的情況。此問題已矯正，可在其他可能情況下進行標記。
- 已驗證說明參考：部分參考材料已過時或指向無效連結。這些情況目前已修正，正確的參考已就位。

Micro Focus Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 將成千上萬個弱點的檢查，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

SSO Bad Practices:Authentication Token Replay

在單一登入程序期間交換的驗證權杖容易受到重新執行攻擊的影響，並可使攻擊者模仿有效使用者以取得未經授權的服務存取權。此版本包含一項檢查，可使用 SAML 通訊協定對 Windows 身分識別框架和服務提供者執行重新執行攻擊。

Cache Management:Headers

HTTP Vary 回應標頭包含一份 HTTP 標頭清單，這些標頭用於決定正確的快取回應，以為傳入的要求提供服務。 Vary 標頭中缺少 'Origin' 時，可使應用程式容易受到用戶端和伺服器端快取破壞攻擊，尤其在提出跨來源要求時。此版本包含一項檢查，可用來偵測 Vary 標頭值中遺失 'Origin' 標頭的情況。

HTML5: CORS Functionality Abuse

若允許來自空來源的 CORS 要求 (即 'Origin: null')，可能危害系統安全性，並使應用程式易於遭受資料竊取。此版本包含一項檢查，可用來偵測伺服器回應中的 Access-Control-Allow-Origin CORS 標頭是否存在 'null' 值。

Insecure Deployment: HTTP Request Smuggling[3]

HTTP Request Smuggling 弱點是因為前端和後端伺服器在剖析不合規 HTTP 標頭時出現差異所導致的。藉由提供一個會由不同伺服器解譯為長度不同的要求，攻擊者就可以毒害後端 TCP/TLS 通訊端，並將任意資料附加到下一個要求的前面，或在前端伺服器不知情的情況下偷傳額外的要求到後端伺服器。本版本包含一項檢查，可用來偵測此弱點。

[3]Insecure Deployment:HTTP Request Smuggling 檢查需要 WebInspect v19.2.0 或更新版本。

Header Manipulation[4]

此版本已增強既有的 Header Manipulation 檢查功能，除了既有的 CRLF 攻擊之外，還納入了歸位字元 ('CR') 和換行字元 ('LF') 攻擊。

合規報告

DISA STIG 4.10

為了在合規領域支援我們的聯盟客戶，此版本包含 WebInspect 檢查與最新版本 Defense Information Systems Agency Application Security and Development STIG 4.10 版之間的關聯性。

原則更新

DISA STIG 4.10

在 WebInspect SecureBase 內現有的支援原則清單中，已新增為納入與 DISA STIG 4.10 相關的檢查而自訂的原則。

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。

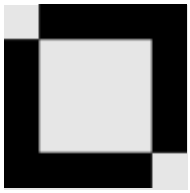
DISA STIG 4.10 和 2019 CWE Top 25

為了呼應新的關聯性，此版本也包含支援 DISA STIG 4.10 和 2019 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。

[4] Header Manipulation 增強功能需要 WebInspect v19.2.0 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 12 月 13 日