Fortify 軟體安全性內容

2024 更新 2
2024 年 6 月 28 日

關於 OpenText Fortify Software Security Research

Fortify Software Security Research 團隊將尖端研究成果轉變爲可爲 Fortify 產品組合 (包括 OpenText™ Fortify Static Code Analyzer 和 OpenText™ Fortify WebInspect) 增添動能的安全情報。現在，Fortify 軟體安全性內容能夠跨 33 種以上的語言支援 1,660 個弱點類別，且涵蓋 100 多萬個單獨 API。

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，2024.2.0 版)、Fortify WebInspect SecureBase (可透過 SmartUpdate 取得)，以及 Fortify Premium Content。

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

隨著此發佈，Fortify Secure Coding Rulepacks 能夠跨 33 種以上的語言偵測 1,435 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：

已改進對 Node.js 的支援 (支援的版本：21.x)[1]

Node.js 是一個跨平台的 JavaScript 執行階段環境，可讓開發人員建立伺服器、Web 應用程式、指令行工具等。此版本包含對 Node.js 支援的重大更新，適用於 Node.js 21.x 中的以下模組：

- async_hooks
- buffer
- child_process
- crypto
- dgram
- dns
- fs
- http
- https
- net
- os
- path
- process
- punycode
- querystring
- stream
- string_decoder
- timers
- tls
- url
- util
- v8
- vm
- worker_threads
- zlib

這些更新改進了以下弱點類別的問題偵測：

- Command Injection
- Dynamic Code Evaluation: Code Injection
- Header Manipulation

[1] 需要 Fortify Static Code Analyzer 24.2 或更高版本。

- Insecure Transport: Weak SSL Cipher
- Insecure Transport: Weak SSL Protocol
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- System Information Leak: External

此外，此版本針對 Node.js 應用程式引入了以下弱點類別：

- DNS Spoofing
- Dynamic Code Evaluation: Script Injection
- Insecure Transport: Insufficient Diffie Hellman Strength
- Key Management: Empty HMAC Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Stream Cipher

已改進對 Java 的支援 (支援的版本：21)

Java 21 是 Java 平台的最新長期支援 (LTS) 版本。它不僅包括對現有 API 的增強，也包括大量的新功能，其中幾個最重要的功能是：外部函數和記憶體 (Foreign Function and Memory)、循序集合 (Sequenced Collections)、金鑰封裝 (Key Encapsulation)、虛擬執行緒 (Virtual Threads)、結構化並行 (Structured Concurrency)、未命名變數 (Unnamed Variables) 和範圍值 (Scoped Values)。在這些功能當中，有些仍處於預覽狀態，但被認爲成熟度已足，可以加入涵蓋範圍。更新的類別包含以下幾類：

- Process Control
- Unreleased Resource
- Weak Encryption
- Weak Cryptographic Hash

此外，還支援以下的新類別：

- Restricted Method
- Weak Cryptographic Signature: XML Signature Secure Validation Disabled

已改進 MyBatis 支援 (支援的版本：3.5. x)

MyBatis 是一個 SQL 對應程式，用於將關聯式資料庫中的物件與物件導向應用程式中的物件相耦合。這個架構使用 XML 描述符號或程式碼註解，將已儲存程序和 SQL 陳述式配對，以簡化開發過程和資料庫通訊。對 MyBatis 的支援已提升至版本 3.5.16。改進項目包括更新對以下弱點類別的支援：

- Dynamic Code Evaluation: Unsafe Deserialization
- SQL Injection
- System Information Leak
- Unreleased Resource: Database
- Unsafe Reflection

MyBatis-Plus 初始支援 (支援的版本：3.5.x)

MyBatis-Plus 建置在現有 MyBatis 架構之上，透過提供有用且高效率並超越原始架構的開箱即用功能來簡化開發。提供了對 MyBatis - Plus 3.5.x 的初始支援。提供對 *SQL Injection* 的初始類別支援。

偵測源自人工智慧 (ML) 和機器學習 (AI) 模型的風險

隨著生成式 AI 和大型語言模型 (LLM) 的使用迅速改變軟體產業的解決方案空間，新的風險也隨之而起。此版本改進了使用 OpenAI API (Python 和 JavaScript)、TensorFlow (Python) 或 Anthropic Claude (Python 和 JavaScript) 的專案涵蓋範圍。支援可偵測因對 AI/ML 模型 API 回應的隱含信任而導致的弱點，還可提供以下功能：

已改進對 OpenAI 的支援 (支援的版本：1.14.x [Python]、4.33.x [JavaScript])

適用於 Python、TypeScript 和 JavaScript 的 OpenAI 程式庫提供了全方位的工具，可用於將進階 AI 功能整合到各種應用程式中。這些程式庫支援各種功能，包括自然語言處理、文字生成和對話式 AI。有了直覺且易於使用的 API，開發人員便可以將 OpenAI 最先進的 AI 模型順暢無礙地內嵌到他們的專案中，從而增強跨 Python、TypeScript 和 JavaScript 環境的互動性與智慧性。改進的支援擴大了 *Cross-Site Scripting: AI* 的涵蓋範圍，並增加了兩個新的弱點類別：

- Cross-Site Scripting: DOM AI
- Prompt Injection

TensorFlow (支援的版本：2.16.x)

TensorFlow 是 Google 開發的領先開放原始碼機器學習架構，提供了一套強大的工具用於建立及部署機器學習模型。這個架構具備內建程式庫和預先訓練模型，簡化了深度學習應用程式的建置。TensorFlow 可針對各種不同的專案集合進行擴充，範圍從研究原型到大規模生產系統。初始涵蓋範圍包含對以下類別的支援：

- Path Manipulation
- Privacy Violation
- System Information Leak: Internal

此外，支援還增加了新的弱點類別：

- Dynamic Code Evaluation: Unsafe TensorFlow Deserialization

Anthropic Claude SDK (支援的版本：0.21.3 [Python]、0.20.5 [JavaScript])

適用於 Python 和 JavaScript 的 Anthropic Claude 程式庫提供了全方位的工具，用於將精密的 AI 語言模型 Claude 整合到應用程式中。初始涵蓋範圍包括對 *Cross-Site Scripting: AI* 的涵蓋範圍，並增加了兩個新的弱點類別：

- Cross-Site Scripting: DOM AI
- Prompt Injection

已改進 Django 支援 (支援的版本： 5.0.x)

Django 是一個使用 Python 編寫的 Web 架構，旨在促進安全、快速的 Web 開發。開發的速度和安全性是透過架構中的高度抽象化來實現的，其中使用程式碼建構與產生來大幅減少樣板程式碼。在此版本中，我們更新了現有的 Django 涵蓋範圍以支援最高版本 5.0.x。

這些更新改進了以下弱點類別的問題偵測：

- Access Control: Database
- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Cross-Frame Scripting
- Cross-Site Request Forgery
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Transport
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Privacy Violation: BREACH
- SQL Injection

Paramiko 初始支援 (支援的版本：3.4.x)

Paramiko 是一個 Python 函式庫，用於透過 SSH 連線到機器。Paramiko 提供了一套功能來從開發人員中擷取加密方法。這提供了類似於通訊端程式設計的高階功能，並允許開發人員存取較低階的方法來進行 SSH 連線的微管理組態。初步支援涵蓋以下弱點類別：

- Command Injection
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Cipher
- Password Management: Hardcoded Password
- SSH Misconfiguration: Missing Authentication

已改進對 PHP 的支援 (支援的版本：8.3)

PHP 是一種廣泛使用的通用指令碼語言，最常用於 Web 開發。此版本將 PHP 支援更新至版本 8.3。尤其是，該版包括改進對以下擴充功能的支援：

- DOM (支援的版本：8.3)

  PHP 的 DOM 擴充功能允許在 PHP 中使用文件物件模型對 XML 和 HTML 文件進行操作。對這個程式庫的擴充支援包括改進對 DOM 操作的資料流程支援，以及用於識別 *Setting Manipulation* 弱點的額外涵蓋範圍。

- JSON (支援的版本：8.3)

  PHP 的 JSON 擴充功能允許使用 PHP 授權下編寫並獲得授權的 JSON 剖析器。這項擴充功能的初始支援包括對此擴充功能的資料流程支援。

- OpenSSL (支援的版本：8.3)

  PHP 的 OpenSSL 擴充功能實作了 OpenSSL 程式庫中用於各種加密操作的功能。對此程式庫的擴充支援包括改進對加密金鑰組的資料流程支援。

- Simdjson (支援的版本：8.3)

  PHP 的 Simdjson 擴充擴充實作了 simdjson 專案的 PHP 特定繫結，以提供快速 JSON 解碼。初始支援包括以下適用於 PHP 的新類別：

  - JSON Path Manipulation

已改進對 iOS 的支援 (支援的版本：17)[2]

Apple 的 iOS 和 IPadOS SDK 提供一系列的架構，讓開發人員能打造適用於 Apple iPhone 和 iPad 裝置的行動應用程式。本版包含我們對 Swift 和 Objective-C 的 iOS SDK 支援的累加式更新。新增和更新的規則都延伸了 iOS 17 中以下架構的 API 涵蓋範圍：

- CryptoKit

[2] iOS 17 API 需要 Xcode 15 或更高版本，而 Xcode 則需要 Fortify Static Code Analyzer 23.2 或更高版本。但是，使用 Source Code Analyzer 23.2 建置使用 iOS 17 API 的應用程式時，可能會出現編譯器警告。爲確保有效的編譯和掃描，建議使用 Fortify Static Code Analyzer 24.2 或更高版本。

- Foundation
- Network
- os
- System
- SwiftUI
- UIKit

這些更新改進了以下弱點類別的問題偵測：

- Insecure Transport
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- System Information Leak: External
- System Information Leak: Internal
- Unreleased Resource: Synchronization
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: 使用者控制的 Salt
- Weak Encryption: User-Controlled Key Size

已改進 MISRA C 2012 支援

MISRA 是一個標準組織，爲安全關鍵環境中使用的應用程式開發制訂及維護各種標準，這些環境需要軟體的高完整性或高可靠性。此版本包括對兩個新類別的支援，這些類別與 MISRA C 2012 標準中的兩個強制性指導規則密切相關：

- Undefined Behavior: File Pointer Dereference
- Undefined Behavior: File Pointer Use After Close

密碼規則運算式屬性更新

Fortify Static Code Analyzer 版本 23.1 中引入的密碼規則運算式屬性是可自訂的屬性，這些屬性包含規則運算式，用於指示 Fortify 規則如何符合各種語言的密碼識別碼。在此版本中，我們擴充了 com.fortify.sca.rules.password_regex.global 屬性的預設值，以辨識涉及「secret」一字的密碼識別碼。此外，我們也新增了新規則，以利用密碼規則運算式屬性來分析動態產生的 JSON 字串。因此，客戶可望看到以下類別的跨語言偵測改進：

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Privacy Violation

已改進對 Golang 的支援 (支援的版本：最高 1.21)

Go (又稱 Golang) 是 Google 所創造的一種經過編譯的靜態歸類程式設計語言。它以簡單、效率及強大的並行性支援而聞名，因此成爲建置可擴充 Web 服務、資料傳輸途徑和分散式系統的理想選擇。此版本包括偵測 *Unreleased Resource* 弱點並針對使用 GORM v2 的專案引入新的 *SQL Injection* 偵測。

WordPress API 改進 (支援的版本：最高 6.5) (API 數量：2)

WordPress 應用程式設計介面 (API) 可以分爲多個 API 部分/主題，每個部分/主題都涵蓋一組指定功能所涉及的功能和使用。這些全部構成了所謂的 WordPress API，也就是由整個 WordPress 專案建立的外掛程式/主題/附加介面。此版本增加了對識別以下 API 中問題的初步支援：

- REST API
- Shortcode API

其他勘誤

在此版本中，我們已投入一切資源，來確保我們可以降低誤報問題數、針對一致性完成修改，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：

減少誤報及其他顯著的偵測改進事項

我們在此版本中持續著手移除誤報。客戶可望看到我們進一步移除誤報，以及與以下領域相關的其他顯著改進：

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* – 已減少 ASP.NET 應用程式中的誤報
- *Insecure Transport: Mail Transmission* – 已減少 Java 應用程式中的誤報
- *Password Management: Hardcoded Password* – 已減少 JSON/YAML 檔案中的誤報
- *Unreleased Resource: Streams* – 已減少 Java 應用程式中的誤報
- *Password Management: Hardcoded Password* – 在 Python 應用程式中偵測到與字典類型相關的新問題
- *Password Management: Hardcoded Password* – 在 ASP.NET 應用程式中偵測到與內插字串相關的新問題
- 移除了來自內建 JDK 系統屬性中的許多誤報

類別名稱變更

當弱點類別名稱發生變更時，若將先前掃描與新掃描的分析結果合併，可能會導致類別的增加/移除。

爲了提高一致性，已重新命名以下三種類別：

2024 R1 類別名稱	2024 R2 類別名稱
Access Control: gRPC Authentication Bypass	Access Control: gRPC Fail Open
AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS CloudFormation Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key
AWS Terraform Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key

DISA Control Correlation Identifier (CCI) 第 2 版

Defense Information Systems Agency (DISA) CCI 是一份文件，透過提供一組與單一可操作的陳述式配對的標準識別碼，彌合了高階和低階網路安全指引之間的差距。DISA Application Security and Development STIG 緊密對應到 DISA CCI，其中單一 STIG 控制可以套用於一個或多個 CCI。此版本使對應的 CCI 與先前版本中針對 Fortify Taxonomy 的 STIG 對應的最新更新保持一致。

NIST Special Publication 800-53 修訂版 4 和 5

美國國家標準與技術研究所 (NIST) Special Publication 800-53 是一份文件，提供對資訊系統的安全與隱私控制目錄，整個網路安全領域都可以利用這個目錄來提供有關如何保護系統安全的指引。NIST Special Publication 800-53 與 DISA CCI 緊密對應，其中單一 CCI 可以套用於一個或多個 NIST 800-53 控制。此版本使對應的 NIST 800-53 控制與針對 Fortify Taxonomy 的 DISA CCI 對應的最新更新保持一致。

OWASP Mobile Top 10 2023

如先前公布，在此版本的 Fortify Software Security Content 中，將淘汰 OWASP Mobile Top 10 2023 對應，僅保留更新的 OWASP Mobile Top 10 2024。

將 Software Security Content 版本與 OpenText 版本控制保持一致

下一個版本將包含安全內容版本控制的變更。這將是最後一個遵循「2024 Update 2」命名慣例的 OpenText Fortify Security Content Update 版本。爲了與 OpenText 版本控制標準保持一致，每年每季安排發佈一次版本，並根據年份和季度進行編號；因此，OpenText™ Fortify™ Software Security Content 版本的下一個版本將會是 24.4，表示 2024 年第四季第一個月的版本。

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 在使用 SmartUpdate 立即取得的以下更新中，將數千個漏洞的檢查與引導客戶的原則結合在一起。

弱點支援

Denial of Service: GraphQL

適用於 API 的 GraphQL 查詢語言提供了查詢現有資料的執行階段。GraphQL 架構是由資料物件、其欄位和類型以及它們與其他資料物件的關係所組成的模型。不同資料物件之間的參考可以建立一個循環。攻擊者可以透過製作惡意巢狀式且昂貴的循環查詢來觸發過多的 CPU 和記憶體使用，從而導致 Denial of Service (DoS)。此版本包括了一項檢查功能，可用於偵測 GraphQL 架構中是否有循環參考。

Access Control: Authorization Bypass (CVE-2024-27198)

CVE-2024-27198 已被識別爲 JetBrains 軟體中的嚴重漏洞，構成重大安全威脅。此漏洞凸顯了與驗證機制不足相關的風險，這可能允許未經驗證的攻擊者獲得對受影響系統的管理控制。最新版本包含一項檢查功能，可用於偵測目標伺服器上是否存在此漏洞。

Directory Traversal (CVE-2024-27199)

2023.11.4 之前的 JetBrains TeamCity On-Premises 版本容易受到 Directory Traversal 缺陷的影響，該缺陷以 CVE-2024-27199 來識別。攻擊者可以利用此缺陷略過驗證控制，嚴重威脅系統的完整性和機密性。最新版本包含一項檢查功能，可用於偵測目標伺服器上是否存在此漏洞。

Dynamic Code Evaluation: Unsafe Deserialization (CVE-2023-26360)

Adobe ColdFusion 2018 Update 15 及更早版本以及 2021 Update 5 及更早版本受到 Dynamic Code Evaluation 漏洞 (以 CVE -2023-26360 來識別) 的影響。此漏洞可能導致在目前使用者的環境中執行任意程式碼。利用此問題不需要使用者互動。此版本包含一項檢查功能，可用於偵測目標伺服器上是否存在此漏洞。

Insecure Deployment: Unpatched Application (CVE-2024-32962)

CVE-2024-32962 是與 xml-crypto (適用於 Node.js 的 XML 數位簽章和加密程式庫) 相關的嚴重漏洞。此漏洞在 4.0.0 版本中引入，並已在 6.0.0 版本中解決。出現該漏洞的原因是，在受影響的版本中，預設組態不會檢查簽署者的授權。攻擊者可以透過修改 XML 文件並用惡意私密金鑰產生的簽名取代現有簽名，以將對應的憑證附加到 <KeyInfo/> 元素，藉此利用此漏洞。此版本包含一項檢查功能，可用於偵測使用受影響 xml -crypto 版本的目標伺服器上是否有此弱點。

其他勘誤

在此版本中，我們已投入一切資源，以進一步降低誤報數，並提升客戶稽核問題的能力。客戶還會看到與下列各領域相關回報結果的變更。

Insecure Deployment: OpenSSL

此版本改進了 OpenSSL ChangeCipherSpec Man-in-the-Middle (MitM) 檢查功能，以減少誤報並提高結果的準確性。

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。

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，網址爲：https://vulncat.fortify.com。

聯絡客戶支援

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

連絡 SSR

Alexander M. Hoole
Software Security Research 資深經理
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Software Security Research 經理
OpenText Fortify
pblay@opentext.com
+1 (669) 309-1634