Fortify 軟體安全性內容

2024 更新 1
2024 年 3 月 29 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 (SCA) 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 1,654 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，2024.1.0 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 1,429 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 Angular 的支援 (支援的版本：16.0.0)

Angular 是一個以 TypeScript 爲基礎的免費開放原始碼 Web 應用程式開發架構，專門用於建立 SPA (單頁應用程式)，主要用於前端，以動態、高效率地操縱資料。對 Angular 的支援從版本 11.2.4 已擴充到 Angular 16.0.0 (僅限初始支援)。Angular 結果已經過增強，客戶可望在 *Cross-Site Request Forgery*、*Privacy Violation* 及 *System Information Leak* 等類別方面取得更好的結果。JavaScript DOM 文件以及下列模組皆已擴充涵蓋範圍：

- @angular/common/http
- @angular/core
- @angular/platform-browser

已改進對 PHP 的支援 (支援的版本：8.2)

PHP 是一種廣泛使用的通用指令碼語言，最常用於 Web 開發。最新的 SSR 版本將 PHP 支援更新至版本 8.2。尤其是，該版本包括對以下附加 PHP 基本擴充功能的初步支援：

- Sodium (支援的版本：8.3.1)

  PHP Sodium 擴充功能是 Libsodium 程式庫的一項實作。Sodium 提供加密、解密、簽章、密碼雜湊及其他加密作業的功能。客戶可能會發現與加密和數位簽章相關的其他問題，以及圍繞著 Privacy Violation 問題的變更。

- Zip (支援的版本：1.22.3)

  PHP Zip 擴充功能是 Libzip 程式庫的一項實作。Zip 提供建立、修改及讀取 zip 封存的功能，這是用於完成檔案/資料分組和壓縮的通用結構。此擴充功能的初始支援包括基本檔案系統資料流程特有的 ZipArchive 類別的涵蓋範圍，以及針對以下類別的 PHP 涵蓋範圍擴充：

  - Key Management: Empty PBE Password
  - Path Manipulation: Zip Entry Overwrite

已改進對 Golang 的支援 (支援的版本：1.21)[1]

Go (又稱 Golang) 由 Google 所創造，是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。Go 結合了編譯語言的效能優勢和解譯語言的程式設計簡單性。其簡潔的語法和強大的標準程式庫，讓開發人員能快速編寫健全的程式碼。我們已擴充以下套件的涵蓋範圍：

- context
- crypto/ecdh
- html/template
- net
- reflect
- Runtime
- time

雲端基礎架構即程式碼 (IaC)[2]

已擴充對雲端基礎架構即程式碼的支援。基礎架構即程式碼是透過程式碼 (而非各種手動程序) 來管理和佈建電腦資源的程序。與上述服務組態設定相關的常見問題現在會回報給開發人員。從 Fortify Static Code Analyzer 24.2 開始，將使用新的技術來報告 Azure ARM 和 AWS CloudFormation 組態問題。因此，在合併使用 Fortify Static Code Analyzer 先前版本產生的 FPR 時增刪了一些問題。使用 Fortify Static Code Analyzer 24.2 及更高版本時，需要 2024.1 Rulepack 來防止重複的 IaC 問題。

Azure Resource Manager (ARM) 組態

ARM 是 Azure 的部署和管理服務。ARM 提供了一個管理層，讓您能在 Azure 帳戶中建立、更新及刪除資源。

Amazon Web Services (AWS) CloudFormation 組態

CloudFormation 是 Amazon 提供的一項服務，用於自動佈建和設定 AWS 資源。CloudFormation 讓使用者能使用 JSON 或 YAML 範本管理 AWS 資源。利用這些範本，使用者可以將資源集合 (稱爲堆疊) 當成單一單元來進行建立、刪除及修改。在此版本中，我們報告了有關 AWS CloudFormation 組態的以下額外弱點類別：

- AWS CloudFormation Misconfiguration: Insecure SageMaker Transport
- AWS CloudFormation Misconfiguration: SageMaker Network Isolation Disabled
- AWS CloudFormation Misconfiguration: Weak SecretsManager Generated Password

[1] 爲了獲得最佳結果，請升級至 Fortify Static Code Analyzer 24.2 或更高版本。
[2] 需要 Fortify Static Code Analyzer 24.2 或更高版本。

已改進 Kotlin 支援 (支援的版本：1.9.2)[3]

Kotlin 是一種具有 Java 互通性的通用靜態型別語言。此版本包括對 Kotlin 1.7.2、1.8 和 1.9 中引入之新標準程式庫 API 的更新支援，這些 API 瞄準以下 Kotlin 命名空間：*Jvm.optional*、*math*、*io.path*、*coroutines.cancellation*、*math*、*io.path*、*coroutines.cancellation* 和 *kotlinx.serialization.json*。在現有類別中可能會偵測到其他問題，包括：

- Denial of Service: Regular Expression
- Path Manipulation
- Privacy Violation
- System Information Leak

JavaScript/TypeScript Node.js 改進[4]

我們已更新 Node.js 規則，以便在使用 Fortify Static Code Analyzer 24.2 時利用類型解析功能。這些變更促成 Node.js 應用程式在大多數類別中誤報減少、真陽性提高、發現準確度更高。更具體地說，客戶可以期待與以下 Node.js 模組相關的結果改進：

- child_process
- dgram
- dns
- fs
- http
- https
- net
- querystring
- tls
- url
- util
- v8

對以下 NPM 套件的初步部分支援也包括在內：

- Bluebird
- child-process-promise

已改進 DISA STIG 5.3 支援

爲了在合規領域支援我們的聯盟客戶，已更新 Fortify Taxonomy 與 Defense Information Systems Agency (DISA) Application Security and Development STIG 5.3 版之間的關聯性，納入了以下 45 個額外的 STIG ID：APSC-DV-000010、APSC-DV-000210、APSC-DV-000230、APSC-DV-000240、APSC-DV-000330、APSC-DV-000380、APSC-DV-000390、APSC- DV-000400、APSC-DV-000410、APSC-DV-000430、APSC-DV-000450、APSC-DV-000580、APSC-DV- 000590、APSC-DV-000710、APSC-DV-001120、APSC-DV-001130、APSC-DV-001280、APSC-DV-001290、APSC-DV-001300、APSC-DV-001310、APSC-DV-001320、APSC-DV-001330、APSC-DV-001410、APSC-DV-001520、APSC-DV-

[3] Kotlin 1.9 支援需要 Fortify Static Code Analyzer 24.2 或更高版本。
[4] 需要 Fortify Static Code Analyzer 24.2 或更高版本。

001530、APSC-DV-001540、APSC-DV-001610、APSC-DV-001760、APSC-DV-001770、APSC-DV-001780、APSC-DV-001790、APSC-DV-001795、APSC-DV-001820、APSC-DV-001970、APSC-DV-002290、APSC-DV-002310、APSC-DV-002320、APSC-DV-002410、APSC-DV-002530、APSC-DV-002890、APSC-DV-002950、APSC-DV-002960、APSC-DV-003100、APSC-DV-003310 和 APSC-DV-003320。

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：

- *Access Control: Anonymous LDAP Bind* – 已移除 C/C++ 應用程式中的誤報
- *Command Injection* – 在使用 C 執行階段程式庫函數的 Windows 變體的 C/C++ 應用程式中偵測到新問題
- *Credential Management: Hardcoded API Credentials* – 已移除 YAML 檔案中的誤報
- *Dockerfile Misconfiguration: Dependency Confusion* – 已移除涉及 npm 的 Dockerfile 中的誤報
- *Dynamic Code Evaluation: Code Injection* – 在使用 Azure Cosmos DB API 的 ASP.NET 應用程式中偵測到新問題
- *GCP Terraform Misconfiguration: Insecure Supply Chain* – 已移除 AWS Terraform 組態檔中的誤報
- *Insecure SSL: Server Identity Verification Disabled* – 在使用「Requests」程式庫的 Python 應用程式中偵測到新問題
- *Mass Assignment: Insecure Binder Configuration* – 已移除 ASP.NET MVC 應用程式中的誤報
- *Mass Assignment: Request Parameters Bound into Persisted Objects* – 已移除 Spring 應用程式中的誤報
- *Password Management: Hardcoded Password* – 在 ODBC 連線字串中偵測到新問題
- *Poor Style: Identifier Contains Dollar Symbol ($)* – 已移除 Java 應用程式中的誤報
- *Privacy Violation* – 在使用 Razor Pages 的 ASP.NET 應用程式中偵測到新問題
- *Privacy Violation* – 在 Dart/Flutter 應用程式中偵測到新問題
- *Privacy Violation* – 在使用「csurf」中介軟體和 ExpressJS 程式庫的 JavaScript 應用程式中偵測到新問題
- *String Termination Error* – 在 C/C++ 應用程式中偵測到新問題
- *System Information Leak: External* – 在使用 Razor Pages 的 ASP.NET 應用程式中偵測到新問題
- *System Information Leak: External* – 在 C/C++ 應用程式中偵測到新問題
- *Weak Encryption: Inadequate RSA Padding* – 已移除使用 OpenSSL 的 PHP 應用程式中的誤報
- 已移除 Python Django 應用程式中的各種資料流程誤報

- 在 Java Spring 應用程式中偵測到各種新資料流程問題
- Java 掃描中 main() 進入點出現的各種資料流程問題可能會顯示爲新增和已移除。這也會移除 Kotlin 和 Scala 應用程式中發現的重複項目和不正確的追蹤。

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，已重新命名以下四種類別：

2023 R4 類別名稱	2024 R1 類別名稱
Insecure Cross-Origin Opener Policy	HTML5: Insecure Cross-Origin Opener Policy
Insecure Transport: Client Identity Verification Disabled	Insecure SSL: Server Identity Verification Disabled
Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control	Kubernetes Terraform Misconfiguration: Improper DaemonSet Access Control
Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control	Kubernetes Terraform Misconfiguration: Improper StatefulSet Access Control

淘汰「Header Checking Disabled」類別

此類別已被移除，以避免與其他類似名稱的類別混淆。此類別中先前的規則現在會在以下類別中報告：

- ASP.NET Misconfiguration: Header Checking Disabled
- ASP.NET Misconfiguration: Unsafe Header Parsing

淘汰某些「Dead Code」類別

以下「Dead Code」類別已從標準 Rulepack 中移除：

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: 未使用的欄位
- Dead Code: Unused Method
- Dead Code: Unused Parameter

客戶如果希望繼續看到這些偵測到的漏洞，可以從 Fortify 支援入口網站下載單獨 Rulepack 中的規則。

重新命名及淘汰 OWASP Mobile Top 10 2023

繼 2023 年 9 月發布「OWASP Top 10 Mobile Risks – 2023 年初始版本」之後，這項專案於 2024 年 1 月已完成，並重新命名爲「OWASP Top 10 Mobile Risks – 2024 年最終版本」。因此，此版本包括針對「OWASP Mobile Top 10 Risks 2024」增加及重新命名的對應。對應本身在功能上沒有變更。

在 Fortify Software Security Content 的下一個版本中，將淘汰 OWASP Mobile Top 10 2023 對應，僅保留更新的 OWASP Mobile Top 10 2024。

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

Insecure Deployment: Unpatched Application (CVE-2024-23897)

Jenkins 是一個以 Java 爲基礎的自動化伺服器，用於建置、測試及部署軟體。Jenkins 指令行介面 (CLI) 是 Jenkins 的內建功能，提供與 Jenkins 伺服器互動的方式，並且預設爲啓用。由 CVE-2024-23897 識別的重大檔案讀取漏洞允許 Jenkins 中的任意檔案讀取功能。此漏洞存在於 args4j 程式庫中，這個程式庫是用於剖析提供給 CLI 的指令引數和選項。這個指令剖析器有一個功能，可以用指定檔案的內容取代引數中後面跟著檔案路徑的 at 符號 (@) 字元。受影響的 Jenkins 版本包括 2.441 及更早版本以及 LTS 2.426.2 及更早版本。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 CVE-2024-23897。

Insecure Deployment: Unpatched Application (CVE-2023-22515)

Atlassian Confluence Data Center 和 Confluence Server 是自我管理的解決方案，以提供組織最佳協作實務做法而聞名。由 CVE-2023-22515 識別的嚴重中斷存取控制漏洞允許惡意動作執行者建立未經授權的管理員帳戶，從而授予他們對 Confluence 平台的不受限制存取權限。即使攻擊者欠缺驗證，他們也可以利用 CVE-2023-22515 建立未經授權的管理員帳戶，並獲得對 Confluence 執行個體的存取權限。攻擊者還可以操縱 Confluence 伺服器設定，來暗示設定過程尚未完成。受影響的 Confluence Server 和 Confluence Data Center 版本爲 8.0.0-8.0.4、8.1.0-8.1.4、8.2.0-8.2.3、8.3.0-8.3.2、8.4.0-8.4.2 和 8.5.0-8.5.1。此版本包括一項檢查功能，可偵測目標伺服器上是否存在 CVE-2023-22515。

Insecure Deployment: Unpatched Application (CVE-2023-22518)

由 CVE-2023-22518 識別的重大不正確的授權漏洞，會影響 Atlassian Confluence Data Center 和 Confluence Server。此漏洞允許未經驗證的攻擊者重設 Confluence 並建立 Confluence 執行個體管理員帳戶。使用此帳戶時，攻擊者可執行 Confluence 執行個體管理員可用的所有管理動作，從而導致機密性、完整性和可用性完全喪失。受影響的 Confluence Server 和 Confluence Data Center 版本爲 7.19.16 之前的所有版本，以及版本 8.3.4、8.4.4、8.5.3 和 8.6.1。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 CVE-2023-22518。

OGNL Expression Injection: Double Evaluation (CVE-2023-22527)

由 CVE-2023-22527 識別出的一個嚴重 OGNL Expression Injection 弱點會影響 Atlassian Confluence Server 和資料中心。此弱點會允許未經驗證的攻擊者在容易遭受攻擊的應用程式上執行任意程式碼。受影響的 Confluence Data Center 和 Confluence Server 版本爲 8.0.x、8.1.x、8.2.x、8.3.x、8.4.x 和 8.5.0-8.5.3。此版本包含一項檢查功能，可用於偵測受影響的 Atlassian 伺服器中是否存在此弱點。

合規報告

已改進 DISA STIG 5.3

爲了在合規領域支援我們的聯盟客戶，已更新 Fortify Taxonomy 與 Defense Information Systems Agency (DISA) Application Security and Development STIG 5.3 版之間的關聯性，納入了以下 8 個額外的 STIG ID：APSC-DV-000210、APSC-DV-000230、APSC-DV-000240、APSC-DV-000450、APSC-DV-001280、APSC-DV-001300、APSC-DV-002530 和 APSC-DV-003320。

原則更新

已改進 DISA STIG 5.3

已更新 DISA STIG 5.3 原則，納入了與 DISA STIG 5.3 相關的其他檢查功能。

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。

XPath Injection

此版本改進了 *XPath Injection* 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。

OWASP Mobile Top 10 2024

爲了呼應經過重新命名的 OWASP Mobile Top 10 Risks 2024 關聯性，本版本也包含支援 OWASP Mobile Top 10 2024 的新 OpenText™ Fortify Software Security Center 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。

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 Fortify 客戶支援

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

聯絡 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