Fortify 소프트웨어 보안 콘텐츠

2024 업데이트 1
2024년 3월 29일 금요일

OpenText Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구를 OpenText™ Fortify Static Code Analyzer (SCA) 및 OpenText™ Fortify WebInspect를 포함한 Fortify 제품 포트폴리오를 강화하는 보안 인텔리전스로 변환하는 일을 하고 있습니다. 현재 Fortify 소프트웨어 보안 컨텐츠는 33개 이상의 프로그래밍 언어에서 1,654개의 취약점 범주를 지원하며 적용되는 개별 API는 1백만 개가 넘습니다.

Fortify Software Security Research (SSR) 팀은 Fortify Secure Coding Rulepacks(영어, 버전 2024.1.0), Fortify WebInspect SecureBase(SmartUpdate를 통해 사용 가능) 및 Fortify Premium Content 업데이트를 즉시 사용할 수 있게 되었다는 소식을 기쁜 마음으로 알려 드립니다.

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

이 릴리스에서 Fortify Secure Coding Rulepacks는 33개 이상의 프로그래밍 언어에서 1,429가지 고유 범주의 취약점을 감지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Angular에 대한 지원 개선(지원되는 버전: 16.0.0)

Angular는 SPA(단일 페이지 응용 프로그램) 생성을 전문으로 하는 타입스크립트 기반의 무료 오픈 소스 웹 응용 프로그램 개발 프레임워크이며, 주로 프런트엔드에서 데이터를 동적이고 효율적으로 조작하는 데 사용됩니다. 버전 11.2.4부터 Angular까지 Angular에 대해 지원되는 범위가 16.0.0확장되었습니다(최초 지원만 해당). 고객이 *Cross-Site Request Forgery*, *Privacy Violation* 및 *System Information Leak* 같은 범주에 대해 더 나은 결과를 기대할 수 있도록 Angular 결과가 향상되었습니다. JavaScript DOM 문서와 함께 적용 범위가 확장된 모듈은 다음과 같습니다.

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

PHP에 대한 지원 개선(지원되는 버전: 8.2)

PHP는 웹 개발에 가장 자주 사용되고 널리 사용되는 범용 스크립팅 언어입니다. 최신 SSR 릴리스 업데이트는 PHP 버전 8.2까지 지원합니다. 구체적으로 이번 릴리스에는 다음과 같은 추가 PHP 기본 확장에 대한 최초 지원이 포함됩니다.

- Sodium(지원되는 버전: 8.3.1)

  PHP Sodium 확장은 Libsodium 라이브러리를 구현한 것입니다. Sodium은 암호화, 암호 해독, 서명, 비밀번호 해시 및 기타 암호화 작업에 대한 기능을 제공합니다. 고객은 Privacy Violation 문제에 대한 변경 사항과 함께 암호화 및 디지털 서명과 관련된 추가 문제를 발견할 수 있습니다.

- Zip(지원되는 버전: 1.22.3)

  PHP Zip 확장은 Libzip 라이브러리를 구현한 것입니다. Zip은 파일/데이터 그룹화 및 압축을 수행하는 데 사용되는 일반적인 구조인 zip 아카이브의 생성, 수정 및 읽기에 대한 기능을 제공합니다. 이번 확장의 최초 지원에는 기본 파일 시스템 데이터 흐름과 관련된 ZipArchive 클래스의 적용 범위와 다음 범주에 대한 PHP 적용 범위의 확장이 포함됩니다.

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

Golang에 대한 지원 개선(지원되는 버전: 1.21)[1]

Golang이라고도 하는 Go는 Google에서 만든 컴파일된 정적인 유형의 프로그래밍 언어입니다. 단순성, 효율성 및 동시성에 대해 강력하게 지원하는 것으로 잘 알려져 있어 확장 가능한 웹 서비스, 데이터 파이프라인 및 분산 시스템을 구축하는 데 적합합니다. Go는 컴파일된 언어의 성능 이점과 해석된 언어에서 볼 수 있는 프로그래밍의 용이성이 결합된 언어입니다. 개발자는 간결한 구문과 강력한 표준 라이브러리를 통해 정확한 코드를 빠르게 작성할 수 있습니다. 적용 범위가 확장된 패키지는 다음과 같습니다.

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

클라우드 IaC(코드형 인프라)[2]

클라우드 IaC에 대한 지원 범위가 확대되었습니다. IaC(코드형 인프라)는 다양한 수동 프로세스가 아닌 코드를 통해 컴퓨터 리소스를 관리하고 프로비저닝하는 프로세스입니다. 그리고 이러한 서비스의 구성과 관련된 일반적인 문제가 이제 개발자에게 보고됩니다. Fortify Static Code Analyser 24.2를 기준으로 Azure ARM 및 AWS CloudFormation 구성 문제는 신규 기술을 사용하여 보고됩니다. 이에 따라 이전 버전의 Fortify Static Code Analysis로 생성된 FPR을 병합하는 경우 일련의 추가 및 제거 문제가 발생합니다. Fortify Static Code Analyser 24.2 이상에서는 중복된 IaC 문제를 방지하기 위해 2024.1 Rulepack이 필요합니다.

ARM(Azure Resource Manager) 구성

ARM은 Azure용 배포 및 관리 서비스입니다. Azure 계정에서 리소스를 생성, 업데이트 및 삭제할 수 있는 관리 레이어를 제공합니다.

AWS(Amazon Web Services) CloudFormation 구성

CloudFormation은 AWS 리소스의 프로비저닝 및 구성을 자동화하는 데 사용되는 Amazon 제공 서비스입니다. 사용자는 CloudFormation을 통해 JSON 또는 YAML 템플릿을 사용하여 AWS 리소스를 관리할 수 있으며, 이러한 템플릿을 활용하여 스택이라고 하는 리소스 모음을 단일 단위로 생성, 삭제 및 수정할 수 있습니다. 이번 릴리스에서는 AWS CloudFormation 구성과 관련하여 다음 추가적인 취약성 범주의 보고 정보가 제공됩니다.

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

[1] 최적의 결과를 얻으려면 Fortify Static Code Analyser 24.2 이상으로 업그레이드하십시오.
[2] Fortify Static Code Analyzer 24.2 이상이 필요합니다.

Kotlin에 대한 지원 개선(지원되는 버전: 1.9.2)[3]

Kotlin은 Java와 상호 운용 가능한 범용 정적 형식 언어입니다. 이번 릴리스에서는 Kotlin 네임스페이스용으로 Kotlin 1.7.2, 1.8 및 1.9에 도입된 신규 표준 라이브러리 API 관련 지원이 업데이트되었습니다. *jvm.optional*, *math*, *io.path*, *coroutines.cancellation* 및 *kotlinx.serialization.json*. 다음을 비롯하여 기존 범주에서 추가 문제가 감지될 수 있습니다.

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

JavaScript/TypeScript Node.js 개선 사항[4]

Fortify Static Code Analyser 24.2를 사용하는 경우 유형 처리의 이점을 누릴 수 있도록 Node.js 규칙이 업데이트되었습니다. 이러한 변경 사항에 따라 대부분의 범주에서 Node.js 응용 프로그램의 거짓 긍정이 줄어들고, 참 긍정이 개선되어 결과가 더 정확해졌습니다. 보다 구체적으로 고객은 다음의 Node.js 모듈과 관련하여 향상된 결과를 기대할 수 있습니다.

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

다음 NPM 패키지에 대한 최초 부분 지원도 포함됩니다.

- Bluebird
- child-process-promise

DISA STIG 5.3에 대한 지원 개선

컴플라이언스 영역에서 연방 고객을 지원하기 위해, Fortify Taxonomy와 DISA(Defense Information Systems Agency) Application Security 및 Development STIG 버전 5.3 사이의 상관 관계가 다음 45개의 추가 STIG ID를 포함하도록 업데이트되었습니다. 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-

[3] Kotlin 1.9 지원을 받으려면 Fortify Static Code Analyzer 24.2 이상이 필요합니다.
[4] Fortify Static Code Analyzer 24.2 이상이 필요합니다.

001300, APSC-DV-001310, APSC-DV-001320, APSC-DV-001330, APSC-DV-001410, APSC-DV-001520, APSC-DV-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 및 APSC-DV-003320.

기타 정정표

이번 릴리스에서는 오탐지 문제의 수를 줄이고 일관성을 위해 리팩터링하고 고객이 문제를 감사하는 역량을 향상시킬 수 있도록 리소스를 투자했습니다. 고객은 다음과 관련하여 보고된 문제를 해결하기 위해 변경된 사항도 확인할 수 있습니다.

오탐지 감소 및 감지 기능 관련 기타 주요 개선 사항

이번 릴리스에서는 오탐지를 없애기 위한 노력이 계속되었습니다. 따라서 오탐지가 더욱 감소하며 다음 영역의 감지 기능도 대폭 개선됩니다.

- *Access Control: Anonymous LDAP Bind*–C/C++ 응용 프로그램에서 오탐지 현상 해소
- *Command Injection*–C 런타임 라이브러리 함수의 Windows 변형을 사용하는 C/C++ 응용 프로그램에서 신규 문제 감지
- *Credential Management: Hardcoded API Credentials*–YAML 파일에서 오탐지 현상 해소
- *Dockerfile Misconfiguration: Dependency Confusion*–npm과 관련된 Dockerfiles에서 오탐지 현상 해소
- *Dynamic Code Evaluation: Code Injection*–Azure Cosmos DB API를 사용하는 ASP.NET 응용 프로그램에서 신규 문제 감지
- *GCP Terraform Misconfiguration: Insecure Supply Chain*–AWS Terraform 구성 파일에서 오탐지 현상 해소
- *Insecure SSL: Server Identity Verification Disabled*–`Requests` 라이브러리를 사용하는 Python 응용 프로그램에서 신규 문제 감지
- *Mass Assignment: Insecure Binder Configuration*–ASP.NET MVC 응용 프로그램에서 오탐지 현상 해소
- *Mass Assignment: Request Parameters Bound into Persisted Objects*–Spring 응용 프로그램에서 오탐지 현상 해소
- *Password Management: Hardcoded Password*–ODBC 연결 문자열에서 신규 문제 감지
- *Poor Style: Identifier Contains Dollar Symbol ($)*–Java 응용 프로그램에서 오탐지 현상 해소
- *Privacy Violation*–Razor Pages를 사용하는 ASP.NET 응용 프로그램에서 신규 문제 감지
- *Privacy Violation*–Dart/Flutter 응용 프로그램에서 신규 문제 감지
- *Privacy Violation*–ExpressJS 라이브러리와 함께 `csurf` 미들웨어를 사용하는 JavaScript 응용 프로그램에서 신규 문제 감지
- *String Termination Error*–C/C++ 응용 프로그램에서 신규 문제 감지
- *System Information Leak: External*–Razor Pages를 사용하는 ASP.NET 응용 프로그램에서 신규 문제 감지
- *System Information Leak: External*–C/C++ 응용 프로그램에서 신규 문제 감지
- *Weak Encryption: Inadequate RSA Padding*–OpenSSL을 사용하는 PHP 응용 프로그램에서 오탐지 현상 해소
- Python Django 응용 프로그램에서 다양한 데이터 흐름 오탐지 현상 해소

- Java Spring 응용 프로그램에서 다양한 신규 데이터 흐름 문제 감지
- Java 검사의 main() 진입점에서 나타나는 다양한 데이터 흐름 문제가 신규 문제로 표시되거나 현상이 해소된 것으로 표시될 수 있습니다. Kotlin 및 Scala 응용 프로그램에서 발견된 중복 및 잘못된 추적도 제거됩니다.

범주 이름 변경

취약성 범주 이름이 변경되면 이전 검사의 분석 결과를 새 검사의 분석 결과와 병합할 때 범주가 추가/제거될 수 있습니다.

일관성을 개선하기 위해 다음 4개 범주의 이름이 변경되었습니다.

2023 R4 범주 이름	2024 R1 범주 이름
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

"Header Checking Disabled" 범주 사용 중단

유사한 이름의 다른 범주와의 혼동을 피하기 위해 이 범주가 제거되었습니다. 이제 이 범주의 이전 규칙은 다음으로 보고됩니다.

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

특정 "Dead Code" 범주 사용 중단

다음 "Dead Code" 범주가 표준 Rulepack에서 제거되었습니다.

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: Unused Field
- Dead Code: Unused Method
- Dead Code: Unused Parameter

감지된 이러한 취약점을 계속 확인하려는 고객은 Fortify 지원 포털에서 별도의 Rulepack으로 규칙을 다운로드하면 됩니다.

OWASP Mobile Top 10 2023의 이름 변경 및 사용 중단
2023년 9월 "OWASP Top 10 Mobile Risks - 최초 릴리스 2023"이 출시된 후 프로젝트가 확정되어 2024년 1월 "OWASP Top 10 Mobile Risks - 최종 릴리스 2024"로 이름이 변경되었습니다. 결과적으로 이번 릴리스에는 "OWASP Mobile Top 10 Risks 2024"에 대해 이름이 변경된 추가 매핑이 포함되어 있습니다. 매핑 자체의 기능적인 면에는 변경 사항이 없습니다.

Fortify 소프트웨어 보안 콘텐츠의 다음 릴리스에서는 OWASP Mobile Top 10 2023 매핑 사용이 중단되며, 업데이트된 OWASP Mobile Top 10 2024만 남게 됩니다.

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase는 SmartUpdate를 사용하여 즉시 사용할 수 있는 다음 업데이트에서 고객을 안내하는 정책과 수천 가지의 취약점 검사를 결합합니다.

취약점 지원

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

Jenkins는 소프트웨어를 구축, 테스트 및 배포하는 데 사용되는 Java 기반 자동화 서버입니다. Jenkins CLI(명령줄 인터페이스)는 Jenkins 서버와 상호 작용하는 방법을 제공하는 Jenkins의 내장 기능이며, 기본적으로 활성화됩니다. CVE-2024-23897로 식별된 치명적인 파일 읽기 취약점으로 인해 Jenkins에서 임의 파일 읽기가 가능해집니다. 이 취약점은 CLI에 제공되는 명령 인수와 옵션을 구문 분석하는 데 사용되는 args4j 라이브러리에서 나타납니다. 명령 구문 분석기에는 인수의 파일 경로 뒤에 오는 at(@) 기호 문자를 지정된 파일의 내용으로 바꾸는 기능이 있습니다. 영향을 받는 Jenkins 버전에는 2.441 이하 및 LTS 2.426.2 이하가 포함됩니다. 이번 릴리스에는 대상 서버에서 CVE-2024-23897을 감지하는 검사 기능이 포함되어 있습니다.

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

Atlassian Confluence Data Center 및 Confluence Server는 조직에 협업을 위한 모범 사례를 제공하는 것으로 알려진 자체 관리형 솔루션입니다. CVE-2023-22515로 식별된 치명적인 액세스 제어 취약점으로 인해 악의적인 행위자가 승인되지 않은 관리자 계정을 생성하여 Confluence 플랫폼에 대한 무제한 액세스 권한을 부여할 수 있습니다. 심지어 공격자가 인증하지 않아도 CVE-2023-22515를 활용하여 무단 관리자 계정을 설정하고 Confluence 인스턴스에 대한 액세스 권한을 얻을 수 있습니다. 또한 공격자는 Confluence 서버 설정을 조작하여 설정 프로세스가 완료되지 않았음을 제안할 수 있습니다. 영향을 받는 Confluence Server 및 Confluence Data Center 버전은 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 및 8.5.0-8.5.1입니다. 이번 릴리스에는 대상 서버에서 CVE-2023-22515를 감지하는 검사 기능이 포함되어 있습니다.

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

CVE-2023-22518로 식별된 치명적인 잘못된 인증 취약점은 Atlassian Confluence Data Center 및 Confluence Server에 영향을 미칩니다. 이 취약점으로 인해 인증되지 않은 공격자가 Confluence를 재설정하고 Confluence 인스턴스 관리자 계정을 생성할 수 있습니다. 공격자는 이 계정을 사용하여 Confluence 인스턴스 관리자가 사용할 수 있는 모든 관리 작업을 수행하여 기밀성, 무결성 및 가용성을 완전히 상실할 수 있습니다. 영향을 받는 Confluence Server 및 Confluence Data Center 버전은 7.19.16 이전 버전 모두와 8.3.4, 8.4.4, 8.5.3 및 8.6.1입니다. 이번 릴리스에는 대상 서버에서 CVE-2023-22518을 감지하는 검사 기능이 포함되어 있습니다.

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

CVE-2023-22527로 식별된 심각한 OGNL Expression Injection 취약점은 Atlassian Confluence Server 및 Data Center에 영향을 줍니다. 이 취약점은 인증되지 않은 공격자가 취약한 응용 프로그램에서 임의의 코드를 실행할 수 있도록 허용합니다. 영향을 받는 Confluence Data Center 및 Confluence Server 버전은 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x 및 8.5.0-8.5.3입니다. 이번 릴리스에는 영향을 받는 Atlassian 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

컴플라이언스 보고서

향상된 DISA STIG 5.3

컴플라이언스 영역에서 연방 고객을 지원하기 위해, Fortify Taxonomy와 DISA(Defense Information Systems Agency) Application Security 및 Development STIG 버전 5.3 사이의 상관 관계가 다음 8개의 추가 STIG ID를 포함하도록 업데이트되었습니다. APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000450, APSC-DV-001280, APSC-DV-001300, APSC-DV-002530 및 APSC-DV-003320.

정책 업데이트

향상된 DISA STIG 5.3

DISA STIG 5.3 정책은 DISA STIG 5.3과 관련된 추가적인 검사를 포함하도록 업데이트되었습니다.

기타 정정표

이번 릴리스에서는 오탐지 수를 더 줄이고 고객이 문제를 감사하는 역량을 향상시킬 수 있도록 리소스를 투자했습니다. 고객은 다음 영역에서 보고된 검사 결과를 해결하기 위해 변경된 사항도 확인할 수 있습니다.

XPath 삽입

이번 릴리스에는 오탐지를 줄이고 결과의 정확성을 높이기 위한 *XPath Injection* 검사 개선 사항이 포함되어 있습니다.

Fortify Premium Content

연구팀은 핵심 보안 인텔리전스 제품 이외에도 다양한 리소스를 구축, 확장 및 유지 관리합니다.

OWASP Mobile Top 10 2024

이름이 변경된 OWASP Mobile Top 10 Risks 2024 상관 관계를 동반하기 위해, 이 릴리스에는 OWASP Mobile Top 10 2024를 지원하는 OpenText™ Fortify Software Security Center에 대한 새로운 보고서 번들이 포함되어 있으며 Premium Content의 Fortify 고객 지원 포털에서 다운로드할 수 있습니다.

Fortify Taxonomy: 소프트웨어 보안 오류

Fortify Taxonomy 사이트(https://vulncat.fortify.com)에는 새로 추가된 범주 지원에 대한 설명이 수록되어 있습니다.

Fortify 고객 지원 연락처

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

SSR 연락처

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

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