Fortify 소프트웨어 보안 콘텐츠

2023 업데이트 4
2023년 12월 15일 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 1,657개의 취약점 범주를 지원하며 적용되는 개별 API는 1백만 개가 넘습니다.

Fortify Software Security Research (SSR) 팀은 Fortify Secure Coding Rulepacks(영어, 버전 2023.4.0), 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 1,432가지 고유 범주의 취약점을 감지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Python에 대한 지원 개선(지원되는 버전: 3.12)

동적 입력이 가능하며 효율적인 고급 데이터 구조를 사용할 수 있는 유용한 범용 프로그래밍 언어인 Python은 구조적/객체 지향/기능적 프로그래밍을 비롯한 여러 가지 프로그래밍 패러다임을 지원합니다. 이번 릴리스에서는 Python 표준 라이브러리 API의 변경 사항 지원 범위가 확장되어 지원 적용 범위가 최신 버전 Python까지 확대되었습니다. 다음 모듈의 기존 규칙 적용 범위가 업데이트되었습니다.

- os
- pathlib
- tomllib

Django에 대한 지원 개선(지원되는 버전: 4.2)

Django는 안전하고 신속한 웹 개발을 할 수 있도록 설계되었으며 Python으로 작성된 웹 프레임워크입니다. 개발 속도와 보안은 코드 구성 및 생성을 사용하여 상용구 코드를 대폭 줄이는 프레임워크에서 높은 수준의 추상화를 통해 얻게 됩니다. 이번 릴리스에서는 기존 Django 지원 범위가 업데이트되어 4.0, 4.1, 4.2 릴리스도 지원됩니다.

이처럼 지원 범위가 확대됨에 따라 *asyncio, django.core.cache.backends.base.BaseCache, django.db.models.Model* 및 *django.middleware.security.SecurityMiddleware* 네임스페이스도 지원됩니다. 또한 취약성 범주 지원 범위도 확대되어 이제 다음 범주가 지원됩니다.

- Header Manipulation
- Insecure Cross-Origin Opener Policy
- Resource Injection
- Setting Manipulation

PyCryptodome 및 PyCrypto(지원되는 버전: 3.19.0)

독립형 Python 패키지인 PyCryptodome에서는 포괄적인 암호화 알고리즘 및 프로토콜 컬렉션이 제공됩니다. 이 패키지는 일반 라이브러리보다 더 높은 빈도로 유지 관리할 수 있는 PyCrypto 라이브러리의 확장 버전이라 할 수 있습니다. Python 응용 프로그램에서 보안 통신, 데이터 보호 및 암호화 작업을 구현해야 하는 개발자의 경우 광범위한 암호화 기능을 제공하는 PyCryptodome을 선택하여 다양한 용도로 활용할 수 있습니다.

취약성 범주의 최초 지원 범위에는 다음이 포함됩니다.

- Key Management: Empty Encryption Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded Encryption Key
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Key Management: Unencrypted Private Key
- Password Management: Hardcoded Password
- Password Management: Lack of Key Derivation Function
- Password Management: Password in Comment
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Insufficient Key Size
- Weak Encryption: Stream Cipher
- Weak Encryption: User-Controlled Key Size

ML(기계 학습) 및 AI(인공 지능) 모델에서 발생하는 위험 감지

생성형 AI와 LLM(대규모 언어 모델)이 사용되면서 소프트웨어 업계의 솔루션 분야가 급격히 변화하고 있으며, 그에 따라 새로운 위험도 등장하고 있습니다. Fortify의 최초 지원 대상에는 OpenAI API, AWS(Amazon Web Services) SageMaker, LangChain을 사용하는 Python 프로젝트가 포함됩니다. Fortify는 지원 대상 프로젝트에서 AI/ML 모델 API가 전송하는 응답의 암시적 신뢰로 인해 발생하는 취약성을 감지하며 다음과 같은 고유 기능도 제공합니다.

Python OpenAI API 최초 지원(지원되는 버전: 1.3.8)

OpenAI Python 라이브러리를 활용하는 개발자는 편리하게 OpenAI REST API에 액세스하여 GPT-4, DALL-E 등의 OpenAI 모델과 상호 작용할 수 있습니다. OpenAI API 사용 시에는 응용 프로그램이 OpenAI 모델에 프롬프트를 전송한 후 생성된 응답을 수신할 수 있으며 기존 모델을 미세 조정할 수도 있습니다. OpenAI Python 모듈에서는 ***httpx*** 기반 비동기 요청과 동기 요청의 전송 및 수신 기능이 지원됩니다. 모델에서 위험할 가능성이 있는 출력을 식별하는 작업이 지원되며, 다음과 같은 새로운 범주도 지원됩니다.

- Cross-Site Scripting: AI

Python AWS SageMaker(Boto3) 최초 지원(지원되는 버전: 1.33.9)

Amazon AWS의 방대한 서비스 제품군에 포함된 제품인 AWS SageMaker는 사용자 지정 모델 학습, MLOps를 지원하는 전체 개발 파이프라인 설정 등 다양한 ML 프로젝트를 지원하는 폭넓은 도구 집합을 제공합니다. Amazon의 Python용 SDK(Boto3)를 사용하면 AWS SageMaker를 비롯한 여러 AWS

제품과 통신할 수 있습니다. 모델에서 위험할 가능성이 있는 출력을 식별하는 작업이 지원되며, 다음과 같은 새로운 범주도 지원됩니다.

- Cross-Site Scripting: AI

Python LangChain 최초 지원(지원되는 버전: 0.0.338)[1]

LangChain은 LLM(대형 언어 모델)을 사용하는 응용 프로그램 개발 과정에서 널리 사용되는 오픈 소스 오케스트레이션 프레임워크입니다. LangChain에서 제공하는 도구와 API를 사용하면 챗봇, 가상 에이전트 등의 LLM 기반 응용 프로그램을 더 쉽게 생성할 수 있습니다. 이러한 도구와 API는 Python 및 JavaScript 기반 라이브러리로 제공됩니다. 모델에서 위험할 가능성이 있는 출력 식별, *Path Manipulation* 감지 등의 작업이 지원되며 다음과 같은 새로운 범주도 지원됩니다.

- Cross-Site Scripting: AI

.NET 8 지원(지원되는 버전: 8.0.0)

.NET 7의 후속 버전인 .NET 8은 프로그래머가 표준화된 API 집합을 사용하여 C#, VB 등의 다양한 언어로 응용 프로그램을 작성할 수 있는 무료 크로스 플랫폼 오픈 소스 개발 프레임워크입니다. 이번 릴리스에서는 지원 범위가 최신 버전 .NET으로 확대되어 신규 API와 기존 API의 취약성 감지 기능이 개선되었습니다.

지원 범위 확대에 따라 지원 대상에 포함된 네임스페이스는 다음과 같습니다.

- System.Collections.Frozen
- System.Net.Http.Json
- System
- System.Security
- System.Text
- System.Text.Unicode
- System.Net.Http

Java Simplified Encryption(Jasypt)(지원되는 버전: 1.9.3)

Jasypt(Java Simplified Encryption)는 비밀번호 기반 암호화를 수행하고 스토리지용 비밀번호 다이제스트를 생성하는 데 사용되는 소형 Java 라이브러리입니다. Spring, Wicket, Hibernate 등 널리 사용되는 Java 프레임워크와 Jasypt를 통합할 수 있습니다.

취약성 범주의 최초 지원 범위에는 다음이 포함됩니다.

- Insecure Randomness
- Key Management: Empty PBE Password
- Key Management: Hardcoded PBE Password
- Key Management: Null PBE Password
- Password Management: Lack of Key Derivation Function
- Privacy Violation: Heap Inspection

[1] LangChain은 최신형 프레임워크이므로 프로덕션 환경에서 사용하기 전에 보안 관련 고려 사항을 면밀하게 평가해야 합니다.

- Setting Manipulation
- 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: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Mode of Operation

ECMAScript 2023

ES2023 또는 ES14라고도 하는 ECMAScript 2023는 JavaScript 언어용 ECMAScript 표준의 최신 버전입니다. ES2023의 주요 기능 중 하나인 새로운 array 함수는 끝에서부터 검색할 수 있으며 복사하여 변경할 수 있습니다. ES2023이 지원됨에 따라 모든 관련 JavaScript 취약성 범주의 지원 적용 범위가 ECMAScript 표준의 최신 버전으로 확장되었습니다.

프로토타입 오염

프로토타입 오염(Prototype Pollution)은 JavaScript 응용 프로그램의 취약점 중 하나입니다. 악의적인 사용자는 이 취약점을 이용해 직접 작성한 코드를 실행하면서 비즈니스 논리를 우회하거나 논리 실행 방식을 변경할 수 있습니다.

이번에 업데이트된 규칙은 공격자가 다음 NPM 패키지에서 객체의 프로토타입을 오염시킬 수 있는지 여부를 감지합니다.

- assign-deep
- deap
- deep-extend
- defaults-deep
- dot-prop
- hoek
- lodash
- merge
- merge-deep
- merge-objects
- merge-options
- merge-recursive
- mixin-deep
- object-path
- pathval

Kubernetes 구성

Kubernetes는 컨테이너화된 응용 프로그램 배포, 확장 및 관리 작업 자동화용 오픈 소스 컨테이너 관리 솔루션입니다. 이 솔루션에서 제공하는 컨테이너 중심 인프라 추상화 기능을 활용하면 기본 인프라를 사용하지 않아도 되므로 이식 가능 배포가 지원됩니다. 그와 동시에 복잡한 분산 시스템도 간편하게 관리할 수 있습니다. 확장된 취약성 범주 지원 범위에는 다음 항목이 포함됩니다.

- Kubernetes Misconfiguration: Improper API Server Network Access Control
- Kubernetes Misconfiguration: Improper CronJob Access Control
- Kubernetes Misconfiguration: Improper DaemonSet Access Control
- Kubernetes Misconfiguration: Improper Deployment Access Control
- Kubernetes Misconfiguration: Improper Job Access Control
- Kubernetes Misconfiguration: Improper Pod Access Control
- Kubernetes Misconfiguration: Improper RBAC Access Control
- Kubernetes Misconfiguration: Improper ReplicaSet Access Control
- Kubernetes Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Misconfiguration: Improper StatefulSet Access Control
- Kubernetes Misconfiguration: Insecure Secret Transport
- Kubernetes Misconfiguration: Insufficient Kubelet Logging
- Kubernetes Misconfiguration: Scheduler System Information Leak
- Kubernetes Misconfiguration: Uncontrolled Kubelet Resource Consumption
- Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control
- Kubernetes Terraform Misconfiguration: Improper Deployment Access Control
- Kubernetes Terraform Misconfiguration: Improper Job Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Network Access Control
- Kubernetes Terraform Misconfiguration: Improper RBAC Access Control
- Kubernetes Terraform Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control
- Kubernetes Terraform Misconfiguration: Insecure Secret Transport

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 추가되었습니다.

OWASP Mobile Top 10 Risks 2023

OWASP(Open Worldwide Application Security Project) Mobile Top 10 Risks 2023에서는 모바일 보안 관련 위험에 대한 인지도를 높이고 모바일 응용 프로그램 개발 및 유지 관리 담당자를 지원하기 위해 주요 위험 정보가 제공됩니다. 웹 응용 프로그램 위험을 경감하고자 하는 고객을 지원하기 위해 OWASP Mobile Top 10 2023의 최초 릴리스와 연관된 Fortify Taxonomy가 추가되었습니다.

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.

20.x 이전 Fortify Static Code Analyzer 버전의 사용 중단

2023.3 릴리스 발표에서 언급했듯이, 해당 릴리스는 20.x 이전의 Static Code Analyzer 버전을 지원하는 규칙 팩의 마지막 릴리스였습니다. 이번 릴리스에서는 20.x 이전 Static Code Analyzer

버전에서 Rulepacks가 로드되지 않습니다. 따라서 Rulepacks를 다운로드하거나 Static Code Analyzer 버전을 업그레이드해야 합니다. 향후 릴리스에서는 Static Code Analyzer의 마지막 4개 주 릴리스가 계속 지원됩니다.

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.

- *ASP.NET Misconfiguration: Persistent Authentication* – 형식 인증 서비스를 사용하는 ASP.NET 응용 프로그램의 오탐지 현상 해소
- *Credential Management: Hardcoded API Credentials* –HTTP Bearer 토큰 관련 기밀 검사의 오탐지 현상 해소
- *Credential Management: Hardcoded API Credentials* – Avature API 키 관련 신규 문제 감지
- *Cross-Site Request Forgery* – `Express.js` JavaScript 프레임워크를 사용하는 NodeJS 응용 프로그램의 신규 문제 감지
- *Cross-Site Scripting* – `html/template` 패키지를 사용하는 Go 응용 프로그램의 신규 문제 감지
- *Cross-Site Scripting: Reflected* –`ListControl` 클래스를 사용하는 ASP.NET 응용 프로그램의 오탐지 현상 해소
- *Denial of Service: Format String* – OWASP Top 10 범주로의 잘못된 매핑
- *Insecure Transport* – 개인 사용자 데이터를 처리하는 controller 메서드 관련 ASP.NET 응용 프로그램의 오탐지 현상 해소
- *Insecure Transport: Mail Transmission* –`smtplib.SMTP` 클래스를 사용하는 Python 응용 프로그램의 오탐지 현상 해소
- *Key Management: Hardcoded Encryption Key* –`RSAKeyGenParameterSpec` 클래스를 사용하는 Java 응용 프로그램의 오탐지 현상 해소
- *Link Injection: Missing Validation* –`WKNavigationDel` 프로토콜을 사용하는 Swift 및 Objective-C 응용 프로그램의 오탐지 현상 해소[2]
- *Mass Assignment: Insecure Binder Configuration* –Jakarta EE API를 사용하는 Java 응용 프로그램의 오탐지 현상 해소
- *Password Management: Password in Configuration File* –구성 파일의 오탐지 현상 해소
- *Path Manipulation* – 파일 업로드 시 PHP 응용 프로그램의 신규 문제 감지
- *SQL Injection* – marsdb 데이터베이스를 사용하는 NodeJS 응용 프로그램의 신규 문제 감지
- *SQL Injection: MyBatis Mapper* – MyBatis 매퍼 XML 파일의 신규 문제 감지
- *String Termination Error* – `printf()` 및 해당 변형을 사용하는 C/C++ 응용 프로그램의 오탐지 현상 해소
- *System Information Leak: Incomplete Servlet Error Handling* –Java 응용 프로그램의 오탐지 현상 해소
- *Weak Encryption: Insecure Initialization Vector* –`Pycryptodome` 라이브러리를 사용하는 Python 응용 프로그램의 오탐지 현상 해소
- *Unreleased Resource: Streams* – `java.nio.file` API를 사용하는 Java 응용 프로그램의 오탐지 식별
- 사용자 프로필 정보와 관련된 Visualforce 응용 프로그램의 다양한 데이터 흐름 오탐지

[2] Fortify Source Code Analyser 23.1 이상 필요

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 2개 범주의 이름이 변경되었습니다.

제거된 범주	추가된 범주
Azure ARM Misconfiguration: Insecure DataBricks Storage	Azure ARM Misconfiguration: Insecure Databricks Storage
Azure ARM Misconfiguration: Insecure Redis Enterprise Transport	Azure ARM Misconfiguration: Insecure Redis Transport

Fortify SecureBase [Fortify WebInspect]

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

취약점 지원

Access Control: 관리 인터페이스

이번 릴리스에는 게이트웨이 액추에이터 엔드포인트가 활성화 및 노출되어 있는데 안전하지 않은 상태일 때 Spring Cloud Gateway의 안전하지 않은 구성을 감지하는 검사 기능이 포함되어 있습니다. 엔드포인트가 이러한 상태이면 공격자는 새 경로를 만들어 응용 프로그램 대신 내부 자산이나 중요한 자산 액세스 권한을 확보할 수 있습니다. 그러면 클라우드 메타데이터 키 도용, 내부 응용 프로그램 노출, DoS(서비스 거부) 공격 등이 발생할 수 있습니다.

Expression Language Injection: Spring

Spring Cloud Gateway 버전 3.1.0, 3.0.0~3.0.6 및 3.0.0 이전 버전에는 CVE-2022-22947로 식별된 보안 취약점이 포함되어 있습니다. 이 취약점으로 인해 게이트웨이 액추에이터 엔드포인트가 활성화 및 노출되어 있는데 안전하지 않은 상태일 때 코드 주입 공격이 발생할 수 있습니다. 이번 릴리스에는 영향을 받는 Spring Cloud Gateway 버전을 사용하는 대상 서버에 이 취약점이 있는지 여부를 감지하는 검사 기능이 포함되어 있습니다.

Insecure Deployment: Unpatched Application

TeamCity 온프레미스 서버 버전 2023.05.3 이하에서는 인증 우회가 발생하기 쉽습니다. 그러면 인증되지 않은 공격자가 서버에서 RCE(원격 코드 실행) 권한을 확보할 수 있습니다. 이 취약점은 CVE-2023-42793으로 식별되었습니다. 이번 릴리스에는 대상 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

정보 검색: 문서화되지 않은 API

API 엔드포인트용 설명서가 문서화되어 있지 않거나 제한적으로만 제공되는 경우 보안 취약점 유무 테스트가 충분히 진행되지 않은 공격 표면이 공격자에게 제공될 수 있습니다. 이 경우 공격자가 해당 공격 표면의 정찰을 수행하여 더 이상 사용/유지 관리되지 않는 패치 미적용 엔드포인트를 찾아낸 후 중요한 정보나 위험한 기능 액세스 권한을 확보할 수 있습니다. 이번 릴리스에 포함되어 있는 검사 기능을 사용하면 액세스는 가능하지만 API 사양 문서에는 정의되어 있지 않은 버전 지정 API 엔드포인트를 검색할 수 있습니다.

컴플라이언스 보고서

DISA STIG 5.3

연방 정부 고객의 컴플라이언스 관련 요구를 지원하기 위해, 이번 릴리스에는 DISA(Defense Information Systems Agency)에서 제공하는 응용 프로그램 보안 및 개발 관련 STIG의 최신 버전인 버전 5.3과 관련된 WebInspect 검사 기능이 포함되었습니다.

정책 업데이트

DISA STIG 5.3

DISA STIG 5.3 관련 검사를 포함하도록 사용자 지정된 정책이 WebInspect SecureBase의 지원되는 정책 목록에 추가되었습니다.

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.

Insecure Transport: SSLv3/TLS 재협상 스트림

TLS 1.3은 재협상을 지원하지 않습니다. 이번 릴리스에는 오탐지를 줄이고 결과의 정확성을 높일 수 있도록 개선된 재협상 스트림 주입 검사 기능이 포함되어 있습니다.

HTML5: Cross-Site Scripting Protection

모든 최신 브라우저에서는 X-XSS-Protection 헤더가 더 이상 사용되지 않습니다. 이번 릴리스부터는 누락되거나 잘못 구성된 X-XSS-Protection 헤더 검사를 사용할 수 없습니다.

Fortify Premium Content

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

DISA STIG 5.3 및 OWASP Mobile Top 10 2023

새로운 상관 관계를 뒷받침하기 위해 이번 릴리스에는 DISA STIG 5.3 및 OWASP Mobile Top 10 2023을 지원하는 OpenText™ Fortify Software Security Center용 신규 보고서 번들도 포함되어 있습니다. Fortify 고객 지원 포털의 Premium Content에서 이 번들을 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