Software Security Research 릴리스 발표

Fortify 소프트웨어 보안 콘텐츠

2022 업데이트 3

2022년 9월 30일 금요일

CyberRes Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구를 Fortify Static Code Analyzer (SCA) 및 Fortify WebInspect를 포함한 Fortify 제품 포트폴리오를 강화하는 보안 인텔리전스로 변환하는 일을 하고 있습니다. 현재 Fortify 소프트웨어 보안 컨텐츠는 30개의 프로그래밍 언어에서 1,244개의 취약점 범주를 지원하며 적용되는 개별 API는 1백만 개가 넘습니다.

CyberRes
A Micro Focus Line of Business

Fortify Software Security Research (SSR) 팀은 Fortify Secure Coding Rulepacks(영어, 버전 2022.3.0), 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]

이번 릴리스에서 Fortify Secure Coding Rulepacks는 30개의 프로그래밍 언어에서 1,024가지 고유 범주의 취약성을 감지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

ASP.NET Core 업데이트(지원되는 버전: 6.0)[1]

MVC(Model-View-Controller) 패턴에서 보기는 Razor 마크업에 포함된 C# 프로그래밍 언어를 사용하는 *.cshtml* 파일입니다. Razor 마크업은 클라이언트로 전송되는 웹 페이지를 생성하기 위해 HTML 마크업과 상호 작용하는 코드입니다. 보기는 응용 프로그램의 데이터 표시 및 사용자 상호 작용을 처리합니다. 이제 Fortify Static Code Analyzer 버전 22.2.0 이상에서는 규칙이 보기 내에서 문제 찾기를 지원합니다. 지원에는 다음과 같은 취약성 범주가 포함됩니다.

- ASP.NET MVC Bad Practices: Form Without AntiForgery Token
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Open Redirect
- Privacy Violation
- System Information Leak

Entity Framework Core(지원되는 버전: 6.0)

EF(Entity Framework) Core는 .NET 응용 프로그램을 위한 오픈 소스 데이터 액세스 기술입니다. EF Core를 사용하면 개발자가 .NET 개체를 데이터베이스 스키마에 매핑하고 표준 API 및 LINQ 쿼리를 통해 데이터베이스 작업을 호출할 수 있습니다. 지원에는 다음과 같은 취약성 범주가 포함됩니다.

- Access Control: Database
- ASP.NET Bad Practices: Leftover Debug Code
- Connection String Parameter Pollution
- Insecure Transport: Database
- Password Management: Hardcoded Password
- Setting Manipulation
- SQL injection
- System Information Leak: Overly Broad SQL Logging

---

[1] Fortify Static Code Analyzer 버전 22.2.0 이상이 필요합니다.

GitHub Actions

GitHub Actions는 빌드, 테스트 및 배포 파이프라인을 자동화할 수 있는 CI/CD(지속적 통합 및 지속적 전달) 플랫폼입니다. 최근의 취약성은 다양한 시스템에서 명령 삽입 공격 벡터를 유발하는 것으로 밝혀졌습니다. 이번 릴리스에는 다음 범주에서 이 명령 삽입 취약성의 일반적인 인스턴스를 감지하는 적용 범위가 포함됩니다.

- Command Injection: GitHub Actions

React(지원되는 버전: 18.2)[2]

React 또는 ReactJS는 구성 요소 기반 사용자 인터페이스를 구축하기 위한 오픈 소스 JavaScript 라이브러리입니다. 이번 릴리스에서는 새로운 취약성 범주가 지원되지 않지만 React의 정확성을 높이고 오탐지를 줄이도록 적용 범위가 리팩터링되었습니다.

React Native(지원되는 버전: 0.70)[2]

React Native는 JavaScript 및 JSX로 다중 플랫폼 사용자 인터페이스를 개발하기 위한 오픈 소스 UI 프레임워크입니다. React Native를 사용하면 개발자가 대상 플랫폼 네이티브 렌더링 API로 렌더링되는 모바일 응용 프로그램을 작성하여 세련되고 일관된 사용자 환경을 생성할 수 있습니다. React에 지원되는 취약성 범주 외에도 React Native에는 다음과 같은 취약성 범주가 추가됩니다.

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

React Native Async Storage(지원되는 버전: 1.17)[2]

Async Storage는 커뮤니티 *react-native-async-storage 프로젝트*를 기반으로 하는 React Native용 암호화되지 않은 비동기 키-값 스토리지 라이브러리입니다. Async Storage는 네이티브 iOS 및 Android 플랫폼별 스토리지 메커니즘을 기반으로 추상화를 제공합니다. 지원을 통해 Async Storage를 통한 데이터 흐름과 기존 JavaScript 및 플랫폼/라이브러리별 취약성 범주 보고가 가능합니다.

기밀 검사 개선 사항

기밀 검사는 다양한 소스 코드 및 구성 파일에서 기밀을 찾는다는 개념입니다. Fortify Static Code Analyzer는 모든 파일 유형에 기밀 검사 적용 범위를 적용하므로 코드 언어에 관계없이 특정 기밀을 찾을 수 있습니다. 다음 기밀에 대한 지원이 추가되었으며 다음과 같이 보고됩니다. *Password Management: Hardcoded Password* 또는 *Credential Management Hardcoded API Credentials*:

- HTTP 기본 인증 토큰
- JWT(JSON Web Token)
- NPM(Node Package Manager) 액세스 토큰
- Postman API 키
- PyPI API 토큰

---

[2] Fortify Static Code Analyzer 버전 22.2.0 이상이 필요합니다.

Java 및 Go에 대한 초기 gRPC 지원(지원되는 버전: 1.49.0)

gRPC(Google Remote Procedure Call)는 최신 다중 환경 및 다중 언어 오픈 소스 고성능 RPC 프레임워크입니다. gRPC는 부하 분산, 추적 및 인증을 지원하는 서비스를 연결합니다. 기존 JSON-over-HTTP와 달리 gRPC는 HTTP2를 기반으로 하며 일반적으로 메시지에 바이너리 프로토콜 버퍼(protobuf) 형식을 사용합니다. gRPC 프로젝트의 경우 사용자가 Fortify Static Code Analyzer의 번역 단계에서 .proto 파일 정의에서 생성된 코드를 포함해야 합니다.

다음 취약성 범주를 다루기 위해 Go gRPC v1.49.0에 대한 지원이 추가되었습니다.

- Header Manipulation
- Privacy Violation
- System Information Leak: External

다음 취약성 범주를 다루기 위해 Java gRPC v1.49.0에 대한 지원이 추가되었습니다.

- Denial of Service
- gRPC Metadata Manipulation
- Insecure Transport
- Insecure Transport: gRPC Server Credentials
- Insecure Transport: gRPC Channel Credentials
- Privacy Violation
- Resource Injection
- System Information Leak: External

초기 Flask 지원(지원되는 버전: 2.2.x)

Flask는 Python으로 작성된 웹 프레임워크입니다. 초기에 *Werkzeug* 및 *Jinja* 라이브러리용 래퍼였던 Flask는 가장 인기 있는 Python 웹 응용 프로그램 프레임워크 중 하나가 되었습니다. Python에 대한 Google Cloud Functions 지원을 보완하기 위해 이번 릴리스에는 Flask Response 개체에 대한 지원만 포함됩니다.
지원에는 다음과 같은 취약성 범주가 포함됩니다.

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Permissive SameSite Attribute
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Unenforced Content Security Policy
- Open Redirect

- Privacy Violation
- System Information Leak: External

Google Cloud Functions(지원되는 버전: 403.0.0)

Google Cloud Functions는 클라우드 서비스를 구축하고 연결하기 위한 서버리스 실행 환경입니다. Google Cloud Functions는 API 호출, 데이터베이스 트랜잭션, Cloud Storage로의 파일 업로드 또는 Pub/Sub 주제에 대한 수신 메시지와 같은 사전 정의된 이벤트에 대한 응답으로 코드를 실행할 수 있습니다.
Cloud Functions는 두 가지 제품 버전을 제공합니다. 하나는 원래 버전인 Cloud Functions(1세대)이고 다른 하나는 향상된 특성 세트를 제공하는 *Cloud Run* 및 *Eventarc* 기반 새 버전인 Cloud Functions(2세대)입니다. 이번 릴리스에는 Python의 Google Cloud Functions에 대한 지원과 Java의 Google Cloud Functions에 대한 업데이트된 지원이 포함됩니다.

Python에 지원되는 취약성 범주에는 다음과 함께 Flask API에서 지원하는 범주가 포함됩니다.

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Privacy Violation
- System Information Leak: External

Python Google Cloud Functions의 경우 사용자는 JSON 또는 YAML 클라우드 빌드 파일을 포함해야 합니다. 또는 검사할 때 다음 속성을 설정하면 됩니다.

- *com.fortify.sca.rules.GCPFunctionName*을 함수 이름으로 설정해야 합니다.
- 트리거 유형이 HTTP인 경우 *com.fortify.sca.rules.GCPHttpTrigger*를 `true`로 설정하고 다른 트리거 유형인 경우 `false`로 설정해야 합니다.

2세대 Java Google Cloud Functions에 대한 업데이트된 규칙 지원은 CloudEvents 요청에서 발생하는 위험한 입력의 소스를 식별합니다.

초기 Apollo Server 지원(지원되는 버전: 3.6.8)

Apollo Server는 JavaScript 응용 프로그램에서 GraphQL API를 구축하는 데 사용되는 오픈 소스 GraphQL 서버입니다. 이번 릴리스에는 Apollo Server로 개발된 GraphQL API에서 다음과 같은 취약성 범주 감지를 포함하여 Apollo Server에 대한 초기 GraphQL 서버 지원이 추가되었습니다.

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- Privacy Violation
- System Information Leak: External

IaC(코드형 인프라)

IaC(코드형 인프라)는 다양한 수동 프로세스가 아닌 코드를 통해 컴퓨터 리소스를 관리하고 프로비저닝하는 프로세스입니다. 지원되는 기술에는 GCP, OpenAPI 사양 및 MuleSoft에 배포하기 위한 Terraform 구성이 포함됩니다. 서비스의 구성과 관련된 일반적인 문제가 이제 개발자에게 보고됩니다.

GCP(Google Cloud Platform) Terraform 구성

Terraform은 클라우드 인프라의 구축, 변경 및 버전 관리를 위한 오픈 소스 IaC 도구입니다. Terraform은 HCL(HashiCorp Configuration Language)이라는 자체 선언적 언어를 사용합니다. 클라우드 인프라는 원하는 상태를 설명하기 위해 구성 파일에 코드화되어 있습니다. Terraform 공급자는 GCP 인프라의 구성 및 관리를 지원합니다. 이번 릴리스에는 GCP Terraform 구성에 대한 다음과 같은 취약성 범주에 대한 적용 범위가 포함됩니다.

- GCP Terraform Misconfiguration: Cloud SQL Database Publicly Accessible
- GCP Terraform Misconfiguration: Cloud Storage Bucket Uniform Access Disabled
- GCP Terraform Misconfiguration: Compute Engine IP Forwarding Enabled
- GCP Terraform Misconfiguration: Compute Engine Serial Console Enabled
- GCP Terraform Misconfiguration: Compute Engine Shielded VM Option Disabled
- GCP Terraform Misconfiguration: GKE Cluster Node Auto-Repair Disabled
- GCP Terraform Misconfiguration: GKE Cluster Publicly Accessible
- GCP Terraform Misconfiguration: Overly Permissive Role
- GCP Terraform Misconfiguration: Permissive Firewall

OpenAPI 사양

OpenAPI 사양은 HTTP API에 대한 프로그래밍 언어에 구애받지 않는 표준 설명을 정의합니다. OpenAPI 사양을 준수하는 OpenAPI 문서는 JSON 또는 YAML 형식으로 나타낼 수 있습니다. 이 표준은 구현, 문서 또는 네트워크 검사에 액세스하지 않고 서비스의 기능을 정의합니다. 이번 릴리스에는 OpenAPI 구성에 대한 다음 취약성 범주에 대한 적용 범위가 포함되어 있습니다.

- OpenAPI Misconfiguration: Credential Leakage
- OpenAPI Misconfiguration: Empty Global Security Requirement
- OpenAPI Misconfiguration: Empty Operation Security Requirement
- OpenAPI Misconfiguration: Insecure Transport
- OpenAPI Misconfiguration: Missing Error Handling
- OpenAPI Misconfiguration: Missing Global Security Requirement
- OpenAPI Misconfiguration: Missing Operation Security Requirement
- OpenAPI Misconfiguration: Missing Security Schemes
- OpenAPI Misconfiguration: Optional Global Security Requirement
- OpenAPI Misconfiguration: Optional Operation Security Requirement
- OpenAPI Misconfiguration: Weak Authentication

Mule

Mule Runtime(줄여서 Mule)은 MuleSoft에서 제공하는 엔터프라이즈 서비스 버스 및 통합 프레임워크입니다. Mule을 사용하면 웹 서비스, HTTP, JDBC(Java Database Connectivity) 등의 기존 시스템을 통합할 수 있습니다. 또한 Mule은 기업 네트워크 내에서 또는 인터넷에서 응용 프로그램 간의 전송 시스템 역할을 하여 서로 다른 응용 프로그램이 서로 통신할 수 있게 해 줍니다. 이번 릴리스에는 Mule 구성에 대한 다음과 같은 취약성 범주가 포함되어 있습니다.

- Mule Misconfiguration: Hardcoded Password
- Mule Misconfiguration: Insecure Database Transport
- Mule Misconfiguration: Insecure Transport
- Mule Misconfiguration: Server Identity Verification Disabled

2022 CWE Top 25

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Weaknesses(CWE Top 25)는 2019년에 도입되었으며 SANS Top 25를 대체합니다. 6월에 릴리스된 2022 CWE Top 25는 지난 2년 동안 NVD(National Vulnerability Database)에 보고된 취약성의 빈도 및 심각도를 정규화하는 추론적 공식을 사용하여 결정되었습니다. NVD에서 가장 일반적으로 보고된 치명적인 취약성을 중심으로 감사의 우선 순위를 지정하고자 하는 고객을 지원하기 위해, CyberRes Fortify Taxonomy와 2022 CWE Top 25 사이의 상관 관계가 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.

19.x 이전 Fortify Static Code Analyzer 버전의 사용 중단

2021.4 릴리스에서 관찰된 바와 같이 Fortify Static Code Analyzer의 마지막 4개 주 릴리스는 계속됩니다. 따라서 이번 릴리스는 19.x 이전 Fortify Static Code Analyzer 버전을 지원하는 Rulepacks의 마지막 릴리스입니다. 다음 릴리스에서는 19.x 이전 Fortify Static Code Analyzer 버전에서 Rulepacks가 로드되지 않습니다. 따라서 Rulepacks를 다운로드하거나 Fortify Static Code Analyzer 버전을 업그레이드해야 합니다. 향후 릴리스에서는 Fortify Static Code Analyzer의 마지막 4개 주 릴리스가 계속 지원됩니다.

IaC(코드형 인프라) 취약성 범주 이름 변경

IaC와 관련된 잘못된 구성 및 관행을 감지하기 위한 지원이 계속 발전함에 따라 보안 컨텐츠의 다음 릴리스에는 취약성 범주의 하위 집합에 대한 범주 이름 변경이 포함될 예정입니다(2022 업데이트 4). 취약성 범주 이름 변경이 발생하면 이전 검사를 새 검사와 병합할 때 검사 결과에 범주가 추가/제거됩니다.

취약성 범주에 대한 Fortify Priority Order Metadata 메타데이터 리팩토링

응용 프로그램 보안 도메인이 지속적으로 발전함에 따라 취약성 범주가 기밀성, 무결성, 가용성에 미치는 영향에 대한 총체적 지식과 이해도가 높아지고 있습니다. 보안 컨텐츠의 다음 릴리스에는 취약성 범주 하위 집합에 대한 취약성 메타데이터 필드 "정확도" 및 "영향"에 대한 변경 사항이 포함될 예정입니다(2022 업데이트 4). 취약성 메타데이터 필드가 변경되면 향후 검사 결과에 다른 필터 집합 폴더에서 문제가 나타날 수 있습니다(예: 중요, 높음, 중간, 낮음). 초기 업데이트로 인해 일부 문제는 상위 FPO(Fortify Priority Order) 폴더에서 하위 FPO 폴더로 이동합니다. 고객은 이러한 변경이 기존 필터 집합 및 템플릿에 어떤 영향을 미칠 수 있는지 파악하고 대비해야 합니다.

오탐지 개선 사항

이번 릴리스에서는 오탐지를 없애기 위한 노력이 계속되었습니다. 기타 개선 사항 외에도, 고객은 다음 영역에서 오탐지가 추가로 사라질 것으로 기대할 수 있습니다.

- *Cross-Site Request Forgery* - 4.5.2 이후 버전의 .NET Framework를 사용하는 .NET 응용 프로그램에서 오탐지 제거
- *JavaScript Hijacking* - 문제(아래 섹션 참조)

- *Key Management* - JavaScript 검사 전반에서 오탐지 감소
- *Key Management* - 주로 SAPUI5 프로젝트에 영향을 미치는 오탐지 감소
- *Key Management* - 비교를 기반으로 한 문제는 많은 오탐지를 생성하므로 제거됨
- *Password Management: Hardcoded/Empty/Null Password* – C# 조건문에 대한 오탐지 방지
- *Password Management* - NPM, Yarn 및 Bower 파일의 오탐지 감소
- *Privacy Violation: Autocomplete* - 새 비밀번호를 설정할 때 오탐지 감소
- *Setting Manipulation* – 환경 변수를 지울 때 오탐지 감소
- *Weak Cryptographic Signature* – java.security 패키지에서 오탐지 방지
- *XML Entity Expansion Injection* – JAXP 변환기를 사용하는 Java 프로그램에서 오탐지 감소

JavaScript Hijacking 제거

다음 범주는 더 이상 최신 ECMAScript와 관련이 없으며 제거되었습니다.

- JavaScript Hijacking
- JavaScript Hijacking: Constructor Poisoning
- JavaScript Hijacking: Vulnerable Framework

결과적으로 위 범주의 모든 문제가 검사 결과에서 제거될 예정입니다.

범주 변경

오탐지 제거와 함께 범주가 통합되어야 하거나 레이블이 잘못 지정된 곳을 일부 식별했습니다. 취약성 범주 이름 변경이 발생하면 이전 검사를 새 검사와 병합할 때 검사 결과에 범주가 추가/제거됩니다.

- *Insecure SSL: Android Hostname Verification Disabled*가 이제 *Insecure SSL:*로 보고됨 *Server Identity Verification Disabled*
- Dockerfile에서 *Password Management: Hardcoded Password* 문제가 이제 *Password Management:*로 보고됨 *Password in Configuration Files*
- .NET에서 데이터베이스 연결 문자열을 설정할 때 Setting Manipulation의 일부 인스턴스가 이제 Connection String Parameter Pollution으로 보고됨

Fortify SecureBase [Fortify WebInspect]

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

취약점 지원

Insecure Deployment: Unpatched Application

dotCMS는 컨텐츠, 이미지 및 자산을 하나의 중앙 위치에서 만들고 재사용할 수 있는 기능을 제공하는 컨텐츠 관리 시스템입니다. ContentResource API는 CVE-2022-26352로 식별되는 RCE(원격 코드 실행) 취약성에 취약합니다. 컨텐츠를 저장하는 데 사용되는 파일 이름은 멀티파트 요청에 제공된 사용자 입력으로 구성되며 dotCMS에 의해 삭제되지 않습니다.

이는 공격자가 시스템에 임의의 파일을 업로드하여 RCE를 감행할 수 있습니다. 이번 릴리스에는 영향을 받는 dotCMS 버전을 실행하는 대상 서버에서 이 취약성을 감지하기 위한 검사 기능이 포함되어 있습니다.

Insecure Deployment: Unpatched Application

Apache APISIX는 로드 밸런싱, 동적 업스트림 등과 같은 트래픽 관리 기능을 제공하는 오픈 소스 API 게이트웨이입니다. 이 API 게이트웨이는 CVE-2022-24112로 식별되는 RCE 취약성에 취약합니다. 공격자는 일괄 요청 플러그인을 통해 Apache APISIX에 대한 IP 제한을 우회할 수 있습니다. APISIX가 기본 Admin 키를 사용하고 Admin API가 활성화되어 있으며 사용자 지정 관리 포트가 할당되지 않은 경우 공격자는 일괄 요청 플러그인을 통해 Admin API를 호출하여 RCE를 감행할 수 있습니다. 이번 릴리스에는 영향을 받는 Apache APISIX 버전을 실행하는 대상 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

Dynamic Code Evaluation: JNDI Reference Injection[3]

JNDI(Java Naming and Directory Interface)는 클라이언트가 이름으로 데이터와 개체를 검색하고 조회할 수 있도록 하는 Java API입니다. 이러한 개체는 RMI(Remote Method Invocation), CORBA(Common Object Request Broker Architecture), LDAP(Lightweight Directory Access Protocol) 또는 DNS(Domain Name Service)와 같은 다양한 이름 지정 또는 디렉터리 서비스를 통해 저장 및 검색할 수 있습니다. 공격자가 JNDI 조회 작업에 대한 인수 제어를 획득할 경우 공격자는 조회 작업이 자신의 제어 하에 있는 명명 또는 디렉토리 서비스를 가리키도록 해 객체 인스턴스화를 위해 원격 팩토리를 사용하는 JNDI 참조를 반환할 수 있습니다. 이 공격은 조회 작업을 수행하는 대상 서버에서 임의의 원격 코드를 실행할 수 있습니다. 이번 릴리스에는 대상 웹 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

Dynamic Code Evaluation: Unsafe Deserialization[3]

Oracle Fusion Middleware 버전 12.2.1.3.0 및 12.2.1.4.0의 ADF Faces 구성 요소에 있는 사전 승인 안전하지 않은 Java 역직렬화 취약성이 CVE-2022-21445로 식별되었습니다. 이는 Business Intelligence, Enterprise Manager, Identity Management, SOA Suite, WebCenter Portal, Application Testing Suite 및 Transportation Management를 포함하여 ADF Faces 구성 요소에 의존하는 모든 응용 프로그램에 영향을 미칩니다. 이 문제로 인해 공격자는 서버에서 임의의 코드를 실행하거나 응용 프로그램 논리를 남용하거나 서비스 거부(DoS) 공격을 시작할 수 있습니다. 이번 릴리스에는 대상 웹 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

컴플라이언스 보고서

2022 CWE Top 25

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Weaknesses(CWE Top 25)는 2019년에 도입되었으며 SANS Top 25를 대체합니다. 6월에 릴리스된 2022 CWE Top 25는 지난 2년 동안 NVD(National Vulnerability Database)에 보고된 취약성의 빈도 및 심각도를 정규화하는 추론적 공식을 사용하여 결정되었습니다.

---

[3] WebInspect 21.2.0.117 이상 패치에서 사용할 수 있는 OAST 기능이 필요합니다.

이 SecureBase 업데이트에는 CWE Top 25로 식별되는 범주에 직접 매핑되거나, "ChildOf" 관계를 통해 Top 25의 CWE-ID와 관계가 설정된 CWE-ID에 매핑되는 검사 기능이 포함되어 있습니다.

정책 업데이트

2022 CWE Top 25

2022 CWE Top 25 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 다음과 관련하여 보고된 검사 결과를 해결하기 위해 변경된 사항도 확인할 수 있습니다.

Dynamic Code Evaluation: Unsafe Deserialization[4]

ID 11504로 식별되는 검사는 OAST 기능을 지원하는 페이로드를 사용하도록 수정되었습니다. 이 검사가 개선되어 오탐지가 줄어들고 결과의 효율성과 정확성이 높아졌습니다.

Fortify Premium Content

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

2022 CWE Top 25

새로운 상관 관계를 뒷받침하기 위해 이 릴리스에는 2022 CWE Top 25를 지원하는 Fortify Software Security Center에 대한 새로운 보고서 번들이 포함되어 있으며 Fortify 고객 지원 포털의 Premium Content에서 다운로드할 수 있습니다.

Fortify Taxonomy: 소프트웨어 보안 오류

Fortify Taxonomy 사이트(https://vulncat.fortify.com)에는 새로 추가된 범주 지원에 대한 설명이 수록되어 있습니다. 마지막으로 지원되는 업데이트가 포함된 기존 사이트를 찾는 고객은 Fortify 지원 포털에서 해당 업데이트를 받을 수 있습니다.

[4] WebInspect 21.2.0.117 이상 패치에서 사용할 수 있는 OAST 기능이 필요합니다.

Fortify 기술 지원 연락처

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR 연락처

Alexander M. Hoole
Software Security Research 수석 관리자
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Manager, Software Security Research
CyberRes Fortify
peter.blay@microfocus.com