Software Security Research 릴리스 발표

Fortify 소프트웨어 보안 콘텐츠

2022 업데이트 2

2022 년 6 월 24 일 금요일

CyberRes Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구 결과를 보안 인텔리전스로 변환하여 Fortify SCA(Static Code Analyzer) 및 Fortify WebInspect 를 포함한 Fortify 제품 포트폴리오를 강화합니다. 현재 Fortify 소프트웨어 보안 컨텐츠는 30 개의 프로그래밍 언어에서 1,220 개의 취약점 범주를 지원하며 적용되는 개별 API 는 1 백만 개가 넘습니다.

Fortify SSR(Software Security Research)은 Fortify Secure Coding Rulepacks(영어, 버전 2022.2.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능) 및 Fortify Premium Content 의 업데이트를 바로 사용할 수 있다는 점을 알려 드립니다.

Fortify Secure Coding Rulepacks [SCA]

이 릴리스에서 Fortify Secure Coding Rulepacks 는 30 개의 프로그래밍 언어에서 1,000 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

.NET 개선 사항(지원되는 버전: 6.0)

.NET 은 프로그래머가 표준화된 API 집합을 사용하여 C# 및 VB.NET 과 같은 언어로 코드를 작성할 수 있도록 하는 일반 프로그래밍 플랫폼입니다. 이번 릴리스에서는 최신 버전의 .NET 으로 적용 범위를 확대하여 데이터 흐름을 개선하고 다음 범주로 API 적용 범위를 확장했습니다.

- Access Control: Database
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- SQL Injection
- System Information Leak: External
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Encryption: Insecure Mode of Operation

ASP.NET Core 개선 사항(지원되는 버전: 6.0)

ASP.NET Core 는 .NET 과 함께 사용하기 위한 주력 웹 프레임워크입니다. 이 프레임워크에는 MVC 웹 응용 프로그램을 비롯한 다양한 유형의 응용 프로그램과 웹 API 를 생성하는 기능이 포함되어 있습니다. 이번 릴리스에서는 적용 범위를 최소 API 를 비롯한 최신 버전의 ASP.NET Core 로 확장하고 다음을 포함하도록 지원되는 범주를 확장했습니다.

- .NET Attribute Misuse: Authorization Bypass
- ASP.NET Bad Practices: Compression Over Encrypted WebSocket Connection
- ASP.NET Middleware Out of Order: Default Cookie Configuration
- ASP.NET Middleware Out of Order: Insecure Transport
- ASP.NET Middleware Out of Order: Insufficient Logging
- ASP.NET Misconfiguration: Insecure Transport
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute

Weak Cryptographic Implementation

Psychic Signatures(CVE-2022-21449)는 Java ECDSA(Elliptical Curve Digital Signature Algorithm) 구현의 취약점입니다. 이 취약점으로 인해 공격자는 응용 프로그램이 모두 0 으로 이루어진 디지털 서명을 유효한 것으로 수락하도록 강제할 수 있습니다. 취약한 Java 버전은 다음과 같습니다. 15, 16, 17, 18. 취약한 버전의 Java 를 사용하는 경우 공격자는 일부 유형의 SSL 인증서, 서명된 JSON 웹 토큰 또는 WebAuthn 인증 메시지를 위조할 수 있습니다. 이번 릴리스에서는 Java 의 *Weak Cryptographic Implementation* 을 보고하는 지원을 추가했습니다.

Jakarta EE 지원(지원되는 버전: 9.0.0)

Jakarta EE 는 클라우드 네이티브 Java 응용 프로그램을 개발하는 데 사용되는 오픈 소스 프레임워크 형태로, 벤더 중립적이고 개방적이며 포괄적인 사양 집합을 제공합니다. 이전에는 Java EE(또는 J2EE)로 알려졌으며 서버 측 Java 용으로 가장 잘 알려진 프레임워크 중 하나였습니다. 이번 릴리스에서는 52 개의 취약점 범주를 아우르는 기존 Java EE 적용 범위에 대한 개선 사항을 추가했습니다.

기밀 검사 개선 사항

기밀 검사는 소스 코드 및 구성 파일에서 기밀을 검색하고 감지하는 기술입니다. 비밀번호나 API 토큰이 포함된 구성 파일이 실수로 소스 코드 리포지토리로 유출되는 경우가 있습니다. 이 릴리스에는 일반적인 비밀번호 해시 형식에 대한 지원이 포함되어 있습니다. 적용 범위에는 다음을 포함한 제품의 구성 파일에 있는 일반적인 비밀번호 해시 형식 및 기밀의 식별이 포함됩니다. OpenVPN, Windows 원격 데스크톱, netrc, IntelliJ IDEA, DBeaver, FileZilla, Heroku, DigitalOcean doctl.
다음 범주에 대한 향상된 적용 범위가 제공됩니다.

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Password Management: Hardcoded Password
- Password Management: Password in Configuration File
- Password Management: Weak Cryptography

Express JS 개선 사항(지원되는 버전: 4.x)[1]

Express 는 Node.js 로 웹 응용 프로그램을 구축하기 위한 프레임워크입니다. 라우팅, 오류 처리, 템플릿, 미들웨어 관리 및 HTTP 관련 유틸리티를 위한 기능을 제공합니다.
이번 릴리스에서는 다음 범주에 대한 Express 4.x 지원을 개선했습니다.

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Insecure Transport
- Path Manipulation

[1] SCA 버전 22.1.1 이 필요함

- Privacy Violation
- Process Control
- Setting Manipulation
- System Information Leak: External

JavaScript Handlebars(지원되는 버전: 4.7.7)

Handlebars 는 재사용 가능한 웹 템플릿을 만들기 위해 설계된 JavaScript 라이브러리입니다. 이러한 템플릿은 HTML, 텍스트 및 표현식의 조합입니다. 표현식은 HTML 코드에 직접 포함되고 코드로 삽입될 컨텐츠에 대한 자리 표시자 역할을 하므로 문서를 쉽게 재사용할 수 있습니다.
이번 릴리스에서는 Handlebars 4.7.7 에 대한 지원을 추가하고, 데이터 흐름 적용 범위를 개선하고, 다음 범주에 대한 API 적용 범위를 확장했습니다.

- Cross-Site Scripting: Handlebars Helper
- Handlebars Misconfiguration: Escaping Disabled
- Handlebars Misconfiguration: Prototypes Allowed
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak
- Template Injection

JavaScript Mustache(지원되는 버전: 4.2.0)

Mustache 는 동적 템플릿을 만들기 위한 기반으로 템플릿과 보기를 제공하는 오픈 소스 논리 없는 템플릿 시스템입니다. 템플릿에는 프레젠테이션 형식과 코드가 포함되는 반면 보기에는 템플릿에 들어갈 데이터가 포함됩니다.
이번 릴리스에서는 *템플릿 삽입* 취약점을 식별하기 위해 Mustache 4.2.0 에 대한 지원을 추가했습니다.

GraphQL.js(지원되는 버전: 16.5.0)

GraphQL.js 는 GraphQL 을 위한 JavaScript 참조 구현이며 JavaScript 응용 프로그램에서 널리 사용됩니다.
이번 릴리스에서는 GraphQL API 의 다음과 같은 취약점 범주를 감지하기 위해 초기 GraphQL 서버 지원을 추가했습니다.

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

Graphene-Python(지원되는 버전: 3.0.0)

Python-Graphene 은 Python 응용 프로그램을 위한 인기 있는 GraphQL 서버 프레임워크입니다. 이번 릴리스에서는 GraphQL API 의 다음 취약점 범주를 감지하기 위해 2022.1.0 의 GraphQL 서버 지원을 개선했습니다.

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

코드형 인프라

IaC(코드형 인프라 Code)는 다양한 수동 프로세스가 아닌 코드를 통해 컴퓨터 리소스를 관리하고 프로비저닝하는 프로세스입니다. 이번 릴리스에서는 IaC 에 대한 확장된 지원을 추가했습니다. 지원되는 기술에는 Azure 및 AWS 배포를 위한 Ansible 구성과 Azure 및 GCP 배포를 위한 Terraform 구성이 포함됩니다. 아래에 나오는 서비스의 구성과 관련된 일반적인 문제가 이제 개발자에게 보고됩니다.

Terraform 구성:

Terraform 은 클라우드 인프라의 구축, 변경 및 버전 관리를 위한 오픈 소스 코드형 인프라 도구입니다. Terraform 은 HCL(HashiCorp Configuration Language)이라는 자체 선언적 언어를 사용합니다. 클라우드 인프라는 원하는 상태를 설명하기 위해 구성 파일에 코드화되어 있습니다.

Terraform 공급자는 ***Microsoft Azure*** 인프라의 구성 및 관리를 지원합니다. 이번 릴리스에서는 Microsoft Azure 서비스 Terraform 구성에 대한 다음 범주를 보고합니다.

- Azure Terraform Misconfiguration: Insecure App Service Transport
- Azure Terraform Misconfiguration: Insecure CDN Endpoint Transport
- Azure Terraform Misconfiguration: Insecure Function App Transport
- Azure Terraform Misconfiguration: Insecure Logic App Transport
- Azure Terraform Misconfiguration: Insecure MariaDB Transport
- Azure Terraform Misconfiguration: Insecure MySQL Transport
- Azure Terraform Misconfiguration: Insecure Network Monitor Transport
- Azure Terraform Misconfiguration: Insecure PostgresSQL Transport
- Azure Terraform Misconfiguration: Insecure Redis Cache Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Redis Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Transport
- Azure Terraform Misconfiguration: Insecure Storage Account Transport

Terraform 공급자는 ***Google Cloud Platform(GCP)*** 인프라의 구성 및 관리를 지원합니다. 이번 릴리스에서는 Google Cloud Platform Terraform 구성에 대한 다음 범주를 보고합니다.

- GCP Terraform Bad Practice: Overly Permissive Service Account
- GCP Terraform Misconfiguration: BigQuery Dataset Publicly Accessible
- GCP Terraform Misconfiguration: Cloud DNS DNSSEC Disabled
- GCP Terraform Misconfiguration: Cloud KMS CryptoKey Publicly Accessible
- GCP Terraform Misconfiguration: Cloud SQL Backup Disabled

- GCP Terraform Misconfiguration: Cloud Storage Bucket Publicly Accessible
- GCP Terraform Misconfiguration: Compute Engine Access Control
- GCP Terraform Misconfiguration: Compute Engine Default Service Account
- GCP Terraform Misconfiguration: Compute Engine Project-Wide SSH
- GCP Terraform Misconfiguration: Google Project Network Access Control
- GCP Terraform Misconfiguration: Insecure Cloud SQL Transport
- GCP Terraform Misconfiguration: Insecure Load Balancer Transport
- GCP Terraform Misconfiguration: Insufficient Cloud Storage Bucket Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Monitoring
- GCP Terraform Misconfiguration: Insufficient VPC Flow Logging
- GCP Terraform Misconfiguration: GKE Cluster Administrative Interface Access Control
- GCP Terraform Misconfiguration: GKE Cluster Certificate-Based Authentication
- GCP Terraform Misconfiguration: GKE Cluster Legacy Authorization
- GCP Terraform Misconfiguration: GKE Cluster HTTP Basic Authentication
- GCP Terraform Misconfiguration: GKE Container-Optimized OS Not In Use
- GCP Terraform Misconfiguration: GKE Node Auto-Upgrade Disabled
- GCP Terraform Misconfiguration: Weak Cryptographic Cloud DNS Signature
- GCP Terraform Misconfiguration: Weak GKE Cluster Network Management
- GCP Terraform Misconfiguration: Weak Key Management

Ansible 구성:
Ansible 은 구성 관리, 응용 프로그램 배포, 클라우드 프로비저닝, 다양한 환경으로 노드 오케스트레이션과 같은 기능을 제공하는 오픈 소스 자동화 기능입니다.

Ansible 에는 ***Amazon Web Services(AWS)***의 구성 및 관리를 지원하는 모듈이 포함되어 있습니다. 이번 릴리스에서는 AWS Ansible 구성에 대한 다음 범주를 보고합니다.

- AWS Ansible Misconfiguration: Amazon RDS Publicly Accessible
- AWS Ansible Misconfiguration: Insecure CloudFront Distribution Transport
- AWS Ansible Misconfiguration: Insufficient CloudTrail Logging

Ansible 에는 ***Microsoft Azure 클라우드 컴퓨팅 서비스***의 구성 및 관리를 지원하는 모듈도 포함되어 있습니다. 이번 릴리스에서는 Microsoft Azure Ansible 구성에 대한 다음 범주를 보고합니다.

- Azure Ansible Misconfiguration: Overly Permissive Azure SQL Database Firewall

기타 정정표

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

Log4j(지원되는 버전: 2.17)

이제 Log4j 에 대한 지원에 새로운 범주인 *Denial of Service: Stack Exhaustion* 이 포함됩니다.

Oslo.config(지원되는 버전: 8.8.0)

Python 용 oslo.config 에 대한 초기 지원에는 새로운 범주인 *Privacy Violation: Unobfuscated Logging* 이 포함되어 있습니다.

Objective-C 오류 수정 및 성능 향상

2022R1 규칙 팩을 사용하여 Objective-C 파일이 포함된 프로젝트를 검사한 고객은 다음과 같은 문제에 직면했을 수 있습니다.

- 검사 단계에서 "[error] Unexpected exception during dataflow analysis..." 데이터 흐름 분석 중 예기치 않은 예외..." 형식의 오류 메시지가 SCA 출력 또는 로그 파일에 나타날 수 있습니다.
- 데이터 흐름 분석 시 검사 시간이 비정상적으로 길어져 데이터 흐름이 손실될 수 있습니다.

이러한 문제를 해결하기 위해 영향을 받는 고객에게 Objective-C 핫픽스 규칙 팩을 제공했습니다. 이 공식 R2 릴리스에는 동일한 수정 사항이 포함되어 있습니다. 핫픽스 규칙 팩을 사용하던 고객은 R2 릴리스 규칙 팩으로 업데이트할 때 핫픽스 규칙 팩을 제거해야 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.

- *SQL Injection: iBatis Data Map* - 리터럴 '$' 문자가 나올 때 오탐지 방지
- *Password Management: Password in Configuration File* - 값이 변수 자리 표시자일 때 오탐지 방지
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property* - [BindRequired] 특성을 사용할 때 C# ASP.NET 응용 프로그램에서 오탐지 방지
- *Often Misused: Authentication* - Java 응용 프로그램에서 오탐지 감소
- *XSS: Content Sniffing* - Java Spring 응용 프로그램에서 오탐지 감소
- *Privacy Violation* - .NET 응용 프로그램에서 오탐지 감소
- *SOQL Injection* 및 *SOSL Injection* - 이제 의미 분석기가 발견한 문제는 낮은 Fortify Priority Order 로 보고됩니다.

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase 는 SmartUpdate 를 통해 즉시 사용할 수 있는 다음 업데이트에서 사용자를 안내하는 정책과 수천 가지의 취약점 검사를 결합합니다.

취약점 지원

OGNL Expression Injection: Double Evaluation

CVE-2022-26134 로 식별된 심각한 OGNL Expression Injection 취약점은 Atlassian Confluence Server 및 Data Center 에 영향을 줍니다. 이 취약점은 인증되지 않은 공격자가 취약한 응용 프로그램에서 임의의 코드를 실행할 수 있도록 허용합니다. 영향을 받는 Confluence Server 및 Data Center 버전은 1.3.0 에서 7.4.16, 7.13.0 에서 7.13.6, 7.14.0 에서 7.14.2, 7.15.0 에서 7.15.1, 7.16.0 에서 7.16.3, 7.17.0 에서 7.17.3 및 7.18.0 입니다. 이번 릴리스에는 영향을 받는 Confluence 및 Data Center 서버에서 취약성을 감지하는 검사 기능이 포함되어 있습니다.

Dynamic Code Evaluation: Code Injection

Pivotal 의 Spring Framework 는 CVE-2022-22965 로 식별된 원격 코드 실행(RCE) 취약성에 취약한 것으로 밝혀졌습니다. 원격 공격자는 임의 코드 실행으로 이어질 수 있는 특수하게 고안된 요청 매개 변수를 제공할 수 있습니다. 이번 릴리스에는 영향을 받는 Spring Framework 버전이 설치된 웹 응용 프로그램에서 이 취약점을 감지하는 검사 기능이 포함되어 있습니다.

Insecure Deployment: OpenSSL

SSL/TLS 연결을 지원하는 데 널리 사용되는 인기 있는 암호화 라이브러리인 OpenSSL 은 CVE-2022-0778 로 식별된 DoS(Denial Of Service) 취약점에 취약한 것으로 밝혀졌습니다. 이로 인해 유효하지 않은 명시적 타원 곡선 매개 변수가 있는 인증서가 생성되어 영향을 받는 시스템에서 무한 루프 DoS 가 트리거될 수 있습니다. 이번 릴리스에는 대상 웹 서버에서 CVE-2022-0778 취약성을 감지하는 검사 기능이 포함되어 있습니다. 이 검사는 영향을 받는 시스템에서 DoS 상태를 일으켜 서비스를 사용할 수 없게 만들 가능성이 있으므로 표준 정책에는 포함되지 않습니다. 모두 검사 정책을 사용하거나 검사를 포함하도록 기존 정책을 사용자 지정하거나 이 검사를 실행하는 사용자 지정 정책을 만드십시오.

기타 정정표

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

Password Management: Weak Password Policy

이번 릴리스에는 입력 유형이 텍스트 상자일 때 향상된 정확도로 비밀번호/사용자 이름 필드가 인식되는 비밀번호 정책 검사에 대한 사소한 개선 사항이 포함되어 있습니다.

Fortify Premium Content

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

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.

Fortify 기술 지원 연락처

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

SSR 연락처

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

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