# Fortify 소프트웨어 보안 콘텐츠

## 2023 업데이트 2
## 2023년 6월 30일 금요일

### OpenText Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구 결과를 토대로 하여 Fortify Static Code Analyzer (SCA) 및 Fortify WebInspect를 포함한 Fortify 제품 포트폴리오를 강화하는 보안 인텔리전스를 파악하고 있습니다. 현재 Fortify 소프트웨어 보안 컨텐츠는 31개 이상의 프로그래밍 언어에서 1,552개의 취약점 범주를 지원하며 적용되는 개별 API는 1백만 개가 넘습니다.

Fortify Software Security Research (SSR) 팀은 Fortify Secure Coding Rulepacks(영어, 버전 2023.2.0), 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 31개 이상의 프로그래밍 언어에서 1,329가지 고유 범주의 취약점을 감지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

### Dart 지원(지원되는 버전: 2.19.6)[1]

Google에서 개발한 Dart 소프트웨어 개발 키트(SDK)에서는 데스크톱, 모바일 및 웹 응용 프로그램을 빌드할 때 사용할 수 있는 안정적 형식의 클래스 기반 가비지 수집 프로그래밍 언어가 제공됩니다. Dart를 사용하는 경우 진행하려는 유스 케이스에 따라 응용 프로그램을 아키텍처별 컴퓨터 코드, 이식 가능 모듈 또는 JavaScript로 컴파일할 수 있으므로 다양한 방식으로 응용 프로그램을 개발할 수 있습니다. Dart를 사용하는 개발자는 Dart에 포함된 그래픽 사용자 인터페이스(GUI)로 응용 프로그램을 만들 수 있습니다. 그러므로 원하는 방식을 유동적으로 선택하여 광범위한 소프트웨어 솔루션을 빌드할 수 있습니다.
지원되는 범주는 다음과 같습니다.

- Access Control: Database
- Command Injection
- Denial of Service
- Denial of Service: Regular Expression
- Header Manipulation
- Insecure Transport
- Open Redirect
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Path Manipulation
- Privacy Violation
- Resource Injection
- Server-Side Request Forgery
- SQL Injection
- System Information Leak
- System Information Leak: Internal

### Flutter 최초 지원(지원되는 버전: 3.7.11)[1]

Google에서 만든 오픈 소스 사용자 인터페이스(UI) SDK이며 Dart 프로그래밍 언어의 기능을 활용하는 Flutter는 개발자가 활용 가능한 포괄적인 도구, 라이브러리 및 패키지 집합을 제공하므로 크로스 플랫폼 응용 프로그램을 원활하게 만들 수 있습니다. Flutter를 사용하는 개발자는 단일 코드베이스에서 모바일, 웹 및 데스크톱 응용 프로그램을 빌드할 수 있으므로 개발 프로세스를 간편하게 진행함으로써 개발 작업 시간과 작업량을 줄일 수 있습니다. 개발자는 Flutter의 기능을 활용해 여러 플랫폼에서 원활하게 실행되는 멋진 디자인과 우수한 성능을 겸비한 응용 프로그램을 만들 수 있습니다. Flutter가 지원됨에 따라 이제 사용자 제공 입력 추적, Dart 프로그래밍 언어용으로 지원되는 모든 범주 감지, 그리고 다음과 같은 Flutter

[1] Fortify Static Code Analyzer 버전 23.1.0이 필요합니다. Fortify Static Code Analyzer 버전 23.1.1 사용 시 최상의 결과가 제공됩니다.

GUI 전용 범주 감지가 가능해졌습니다.

- Privacy Violation: Shoulder Surfing
- System Information Leak: Internal

**Android 13(API 수준: 33)**

Android 플랫폼은 모바일 장치용 오픈 소스 소프트웨어 스택입니다. Android의 기본 구성 요소인 Java API 프레임워크에서는 응용 프로그램 개발자에게 Android 기능을 제공합니다. 이번 릴리스에서는 Android의 Java API 프레임워크를 활용하며 Java나 Kotlin으로 작성된 기본 Android 응용 프로그램의 취약점 감지 기능이 확장되었습니다. 또한 이번 릴리스에는 Android 응용 프로그램용으로 다음의 5가지 신규 취약성 범주가 추가되었습니다.

- Privacy Violation: Android Insecure Indexing
- Privilege Management: Android Nearby Devices
- Privilege Management: Android Notifications
- Privilege Management: Android Read Aural Media
- Privilege Management: Android Read Visual Media

그리고 다음 네임스페이스의 기존 취약성 범주를 감지할 수 있도록 추가 Android 업데이트도 포함되었습니다.

- android.app
- android.content
- android.net
- android.os
- android.util
- java.nio
- java.security
- java.security.interfaces

**Java SE JDK(지원되는 버전: 17)**

Java Platform, Standard Edition(SE) Java 개발 키트(JDK)는 Java 응용 프로그램 및 구성 요소를 개발하는 데 사용되는 도구와 라이브러리가 포함된 소프트웨어 개발 패키지입니다. 이번 릴리스에서는 Java SE JDK 15, 16, 17에 도입된 신규 API를 대상으로 다음 네임스페이스의 기존 취약성 범주 지원이 업데이트되었습니다.

- java.io
- java.lang
- java.lang.reflect
- java.net
- java.nio.channels
- java.util
- java.util.random
- java.util.stream

또한 스캔 적용 범위도 확대되어 다음 범주에서 확인된 추가적인 문제도 스캔이 가능할 수 있습니다.

- Insecure Randomness
- Insecure Randomness: Hardcoded Seed
- Insecure Randomness: User-Controlled Seed
- Server-Side Request Forgery
- Setting Manipulation
- Unsafe Reflection

### Kotlin 표준 라이브러리 업데이트(지원되는 버전: 1.7.21)

Kotlin은 Java와 상호 운용 가능한 범용 정적 형식 언어입니다. 이번 릴리스에서는 Java Virtual Machine(JVM)용으로 Kotlin 버전 1.6과 1.7에 도입된 신규 표준 라이브러리 API 관련 지원이 업데이트되었습니다.

### 기밀 검사 업데이트

기밀 검사는 소스 코드 및 구성 파일에서 기밀을 자동으로 검색하는 기술입니다. 여기서 "기밀"이란 비공개 상태로 유지해야 하는 비밀번호, API 토큰, 암호화 키 및 이와 유사한 아티팩트를 지칭합니다. 이번 릴리스에서는 다음 범주의 기밀 검사 지원이 업데이트되었습니다.

- Credential Management: Hardcoded API Credentials
- Key Management: Hardcoded Encryption Key
- Password Management: Hardcoded Password

또한 이제는 다음 범주에서 PowerShell 스크립트를 통한 기밀 검사가 지원됩니다.

- Password Management: Hardcoded Password
- Privacy Violation

### 클라우드 IaC(코드형 인프라)

IaC(코드형 인프라)는 다양한 수동 프로세스가 아닌 코드를 통해 컴퓨터 리소스를 관리하고 프로비저닝하는 프로세스입니다. 이번 릴리즈에서는 지원되는 기술 범위가 확장되어 Amazon Web Services(AWS) 및 Google Cloud Platform(GCP) 배포용 Terraform 구성 및 AWS CloudFormation용 구성이 모두 지원됩니다. 그리고 이러한 서비스의 구성과 관련된 일반적인 문제가 이제 개발자에게 보고됩니다.

#### AWS 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 AWS 인프라의 구성 및 관리를 지원합니다. 이번 릴리스에서는 Terraform 구성과 관련하여 다음 범주의 보고 정보가 제공됩니다.

- AWS Terraform Misconfiguration: Aurora Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: CloudWatch Missing Customer-Managed Encryption Key

- AWS Terraform Misconfiguration: Database Migration Service Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: DocumentDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: ElastiCache Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Improper API Gateway Access Control
- AWS Terraform Misconfiguration: Improper EC2 Network Access Control
- AWS Terraform Misconfiguration: Improper ECR Access Control
- AWS Terraform Misconfiguration: Improper EKS Network Access Control
- AWS Terraform Misconfiguration: Improper ElastiCache Network Access Control
- AWS Terraform Misconfiguration: Improper Lambda Access Control
- AWS Terraform Misconfiguration: Improper MSK Network Access Control
- AWS Terraform Misconfiguration: Improper Neptune Access Control
- AWS Terraform Misconfiguration: Improper RDS Network Access Control
- AWS Terraform Misconfiguration: Improper S3 Access Control
- AWS Terraform Misconfiguration: Improper VPC Network Access Control
- AWS Terraform Misconfiguration: Insecure API Gateway Storage
- AWS Terraform Misconfiguration: Insecure API Gateway Transport
- AWS Terraform Misconfiguration: Insecure App Sync Storage
- AWS Terraform Misconfiguration: Insecure Athena Storage
- AWS Terraform Misconfiguration: Insecure CloudFront Transport
- AWS Terraform Misconfiguration: Insecure DynamoDB Storage
- AWS Terraform Misconfiguration: Insecure EC2 Storage
- AWS Terraform Misconfiguration: Insecure ECR Storage
- AWS Terraform Misconfiguration: Insecure ECS Transport
- AWS Terraform Misconfiguration: Insecure EKS Storage
- AWS Terraform Misconfiguration: Insecure ElastiCache Storage
- AWS Terraform Misconfiguration: Insecure Glue Storage
- AWS Terraform Misconfiguration: Insecure Kinesis Storage
- AWS Terraform Misconfiguration: Insecure MQ Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Transport
- AWS Terraform Misconfiguration: Insecure RDS Transport
- AWS Terraform Misconfiguration: Insecure S3 Storage
- AWS Terraform Misconfiguration: Insecure SageMaker Storage
- AWS Terraform Misconfiguration: Insufficient API Gateway Logging
- AWS Terraform Misconfiguration: Insufficient Aurora Backup
- AWS Terraform Misconfiguration: Insufficient CloudFront Logging
- AWS Terraform Misconfiguration: Insufficient CloudTrail Logging
- AWS Terraform Misconfiguration: Insufficient EC2 Logging
- AWS Terraform Misconfiguration: Insufficient ELB Logging
- AWS Terraform Misconfiguration: Insufficient ElastiCache Backup
- AWS Terraform Misconfiguration: Insufficient ElastiCache Logging
- AWS Terraform Misconfiguration: Insufficient Global Accelerator Logging
- AWS Terraform Misconfiguration: Insufficient GuardDuty Monitoring
- AWS Terraform Misconfiguration: Insufficient Lambda Logging
- AWS Terraform Misconfiguration: Insufficient OpenSearch Service Logging
- AWS Terraform Misconfiguration: Insufficient RDS Backup
- AWS Terraform Misconfiguration: Insufficient Redshift Logging
- AWS Terraform Misconfiguration: Insufficient S3 Backup
- AWS Terraform Misconfiguration: MemoryDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: MQ Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Neptune Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Reduced CloudFront Availability

- AWS Terraform Misconfiguration: Reduced ELB Availability
- AWS Terraform Misconfiguration: Reduced StackSets Availability
- AWS Terraform Misconfiguration: Weak Cognito Authentication
- AWS Terraform Misconfiguration: Weak IAM Password Policy

**GCP Terraform 구성**

Terraform은 클라우드 인프라 빌드, 변경 및 버전 관리용 오픈 소스 코드형 인프라 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 릴리스에서는 GCP Terraform 구성과 관련하여 다음 취약성 범주의 보고 정보가 제공됩니다.

- GCP Terraform Misconfiguration: Insufficient Cloud Load Balancing Logging
- GCP Terraform Misconfiguration: Insufficient Cloud NAT Logging
- GCP Terraform Misconfiguration: Insufficient Media CDN Logging
- GCP Terraform Misconfiguration: Insufficient Operations Suite Logging

**AWS CloudFormation 구성**

CloudFormation은 AWS 리소스의 프로비저닝 및 구성을 자동화하는 데 사용되는 Amazon 제공 서비스입니다. CloudFormation 사용자는 JSON 또는 YAML 템플릿을 사용하여 AWS 리소스를 관리할 수 있습니다. 이번 릴리스에서는 AWS CloudFormation 구성과 관련하여 다음 취약성 범주의 보고 정보가 제공됩니다.

- AWS CloudFormation Misconfiguration: AmazonMQ Publicly Accessible
- AWS CloudFormation Misconfiguration: Backup Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: CloudTrail Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DataBrew Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Publicly Accessible
- AWS CloudFormation Misconfiguration: DocDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DocDBElastic Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DynamoDB Backup Disabled
- AWS CloudFormation Misconfiguration: EC2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ECR Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FinSpace Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FSx Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ImageBuilder Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Improper Athena Access Control
- AWS CloudFormation Misconfiguration: Improper CodeStar Access Control
- AWS CloudFormation Misconfiguration: Improper Cognito Access Control
- AWS CloudFormation Misconfiguration: Improper ECS Network Access Control
- AWS CloudFormation Misconfiguration: Improper EMR Access Control
- AWS CloudFormation Misconfiguration: Improper KMS Access Control
- AWS CloudFormation Misconfiguration: Improper Lambda Network Access Control
- AWS CloudFormation Misconfiguration: Improper Lightsail Access Control
- AWS CloudFormation Misconfiguration: Improper M2 Access Control

- AWS CloudFormation Misconfiguration: Improper QLDB Access Control
- AWS CloudFormation Misconfiguration: Improper RDS Access Control
- AWS CloudFormation Misconfiguration: Improper Redshift Access Control
- AWS CloudFormation Misconfiguration: Improper S3 Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Network Access Control
- AWS CloudFormation Misconfiguration: Improper Serverless Network Access Control
- AWS CloudFormation Misconfiguration: Improper Transfer Network Access Control
- AWS CloudFormation Misconfiguration: Insecure API Gateway Transport
- AWS CloudFormation Misconfiguration: Insecure CloudFront Transport
- AWS CloudFormation Misconfiguration: Insecure DAX Storage
- AWS CloudFormation Misconfiguration: Insecure ECR Supply Chain
- AWS CloudFormation Misconfiguration: Insecure EFS Storage
- AWS CloudFormation Misconfiguration: Insecure ELB Transport
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Storage
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Transport
- AWS CloudFormation Misconfiguration: Insecure WorkSpaces Storage
- AWS CloudFormation Misconfiguration: Insufficient API Gateway Logging
- AWS CloudFormation Misconfiguration: Insufficient AppSync Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Monitoring
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Config Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ECR Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ELB Logging
- AWS CloudFormation Misconfiguration: Insufficient ElasticLoadBalancing Logging
- AWS CloudFormation Misconfiguration: Insufficient Elasticsearch Logging
- AWS CloudFormation Misconfiguration: Insufficient GuardDuty Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Lambda Logging
- AWS CloudFormation Misconfiguration: Insufficient MQ Logging
- AWS CloudFormation Misconfiguration: Insufficient MSK Logging
- AWS CloudFormation Misconfiguration: Insufficient OpenSearch Service Logging
- AWS CloudFormation Misconfiguration: Insufficient RDS Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Route 53 Logging
- AWS CloudFormation Misconfiguration: Insufficient Serverless Logging
- AWS CloudFormation Misconfiguration: Insufficient Stack Monitoring
- AWS CloudFormation Misconfiguration: Kinesis Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Lambda Denial of Service
- AWS CloudFormation Misconfiguration: Location Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Logs Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: M2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: MemoryDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Neptune Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Privileged Batch Container
- AWS CloudFormation Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: RDS Publicly Accessible
- AWS CloudFormation Misconfiguration: Redshift Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Reduced EC2 Availability
- AWS CloudFormation Misconfiguration: Reduced ElastiCache Availability

- AWS CloudFormation Misconfiguration: Reduced Stack Availability
- AWS CloudFormation Misconfiguration: Rekognition Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: S3 Backup Disabled
- AWS CloudFormation Misconfiguration: SQS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: SageMaker Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Serverless Denial of Service
- AWS CloudFormation Misconfiguration: Timestream Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Weak API Gateway Authentication
- AWS CloudFormation Misconfiguration: Weak Certificate Manager Authentication
- AWS CloudFormation Misconfiguration: Weak IAM Authentication
- AWS CloudFormation Misconfiguration: Weak Lambda Authentication
- AWS CloudFormation Misconfiguration: Weak RDS Authentication

### 사용자 지정 가능 비밀번호 관리 정규식 업데이트

이제 다음 속성을 사용하여 Salesforce Apex, Dart 및 PowerShell 스크립트용으로 사용자 지정 가능 비밀번호 관리 정규식을 지정할 수 있습니다.

- com.fortify.sca.rules.password_regex.apex
- com.fortify.sca.rules.password_regex.dart
- com.fortify.sca.rules.password_regex.powershell

이러한 속성을 사용하면 Salesforce Apex 소스 코드, Dart 소스 코드 또는 PowerShell 스크립트를 스캔할 때 비밀번호 식별에 사용되는 기본 정규식을 다시 정의할 수 있습니다.

### OWASP Mobile Application Security Verification Standard(MASVS) v2.0.0

OWASP Mobile Application Security(MAS) 프로젝트의 일환으로 2023년 4월에 공개된 OWASP MASVS v2.0.0 표준은 모바일 응용 프로그램 보안 요구 사항의 기준을 제공합니다. 모바일 소프트웨어 설계자, 개발자, 테스터 등이 이 표준을 사용할 수 있습니다. OWASP MASVS 2.0은 모바일 장치에서 실행되는 "클라이언트" 모바일 응용 프로그램의 보안 관련 요구 사항을 중점적으로 제시합니다. 따라서 이 버전을 OWASP ASVS와 함께 사용하여 원격 엔드포인트 제어와 관계가 있는 관련 서버 쪽 응용 프로그램의 보안 위험을 평가해야 합니다. 이번 릴리스에서는 안전한 모바일 응용 프로그램을 개발하고 모바일 응용 프로그램의 보안 제어 적용 범위 및 위험 완화를 평가하는 Micro Focus 고객을 지원하기 위해 OWASP MASVS v2.0.0 버전과 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.

### *"Access Control" 범주 사용 중단*

이번 릴리스에서는 Salesforce Apex용 *Access Control* 범주가 제거되었습니다. 이에 따라 필드 수준 보안 확인 기능이 제공되지 않습니다. 이제는 *Access Control: Database* 및 *SOQL Injection* 등의 기타 범주를 통해 필드 수준 보안 문제를 간접적으로 파악할 수 있습니다.

### *"Link Injection: Auto Dial" 범주 사용 중단*

최신 정보를 제공하지 않는 *Link Injection: Auto Dial* 범주가 제거되었습니다. 이 범주는 CVE-2017-2484 취약점(공격자가 iOS 앱에서 정화되지 않은 사용자 입력을 악용해 특정 전화 번호에 자동으로 전화를 걸거나 Facetime 통화를 시도할 수 있음) 해결을 위해 도입되었습니다. 이러한 악용 문제는 iOS 10.3 업데이트에서 해결되었으므로 최신 iOS 앱에서는 더 이상 발생하지 않습니다.

### *사용이 중단된 표준 매핑*

다음 표준과 모범 사례는 더 이상 사용되지 않는 항목으로 표시되었으므로 이제 기본적으로 표시되지 않습니다.

- CWE Top 25 2019
- CWE Top 25 2020
- DISA STIG 4.9
- DISA STIG 4.10
- OWASP Top 10 2004
- OWASP Top 10 2007
- OWASP Top 10 2010
- SANS Top 25 2009
- SANS Top 25 2010
- WASC 24 + 2

### *PHP 동적 함수* [2]

최신 Fortify Static Code Analyzer에서 PHP 지원이 업데이트됨에 따라, 정화되지 않은 외부 입력이 참조하는 동적 함수를 대상으로 *Dynamic Code Evaluation: Code Injection* 문제 보고가 지원됩니다.

### *Java의 Unsafe 클래스*

Java JDK 내에는 기본적으로 안전하지 않은 작업을 수행할 때 사용되는 숨김 클래스가 있습니다. 이 클래스는 인스턴스화하려면 리플렉션을 수행해야 하므로 대개 개발자는 사용할 수 없습니다. 하지만 이제는 Java 프로젝트 내에서 `sun.misc.Unsafe` 클래스를 사용할 때 스캔 결과에서 해당 클래스의 모든 사용이 *Often Misused: sun.misc.Unsafe*로 보고됩니다.

[2] SCA 버전 23.1 이상이 필요합니다.

### *오탐지 개선 사항*

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

- *Access Control: Unenforced Sharing Rules* – Salesforce 트리거, Visualforce 페이지 및 구성 요소에서 오탐지 제거
- *Command Injection* – JavaScript에서 정규식에 플래그를 지정할 때 발생하는 오탐지 제거
- *Cookie Security: Cookie not Sent Over SSL* – 권장 수정 사항 적용 시 Swift에서 발생하는 오탐지 제거
- *Credential Management: Hardcoded API Credentials* – 전달자 토큰 식별 시에 발생하는 오탐지 제거
- *Dead Code: Expression is Always false* – Java 스위치 문에 표시될 때 발생하는 오탐지 제거
- *Dockerfile Misconfiguration: Dependency Confusion* – dockerfile 내의 "apt" 및 "apt-get" 명령 관련 오탐지 제거
- *Log Forging (debug)* – HTTP 요청 헤더 값을 인쇄할 때 Salesforce Apex 응용 프로그램에서 발생하는 오탐지 제거
- *Race Condition:* Signal Handling – `sigaction()` 호출 시 C/C++에서 발생하는 오탐지 제거
- *String Termination Error* – C++에서 기본 형식을 트리거할 때 발생하는 오탐지 제거
- *Unused Method* – 구현된 Serializable 메서드가 다른 메서드를 호출하는 Java 코드의 오탐지 제거
- 부울 값에서 트리거되었을 수 있는 JavaScript의 데이터 흐름 오탐지 제거

### *범주 변경*

취약성 범주 이름 변경이 발생하면 이전 검사를 새 검사와 병합할 때 분석 결과에 범주가 추가/제거됩니다.

일관성을 개선하기 위해 다음 범주의 이름이 변경되었습니다.

- *Azure Terraform Misconfiguration: Improper CosmosDB CORS Policy*가 이제 *Azure Terraform Misconfiguration: Improper Cosmos DB CORS Policy*로 보고됨
- *Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller*가 이제 *Kubernetes Misconfiguration: Missing Service Account Admission Controller*로 보고됨
- *NoSQL Injection: CosmosDB*가 이제 *NoSQL Injection: Cosmos DB*로 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:**

엔터프라이즈 모바일 및 웹 응용 프로그램을 만드는 데 사용되는 오픈 소스 Java 라이브러리인 ZK 프레임워크에는 CVE-2022-36537로 식별된 보안 취약점이 포함되어 있습니다. 공격자는 이 취약점을 악용하여 웹 컨텍스트에 있는 파일의 내용을 검색할 수 있습니다. 해당 취약점을 정상적으로 악용한 공격자는 중요한 정보를 입수하거나 일반적으로는 연결이 불가능한 엔드포인트를 대상으로 공격을 실행할 수 있습니다. 이번 릴리스에는 영향을 받는 ZK 프레임워크 버전을 사용하는 대상 서버에서 이 취약점을 감지하기 위한 검사 기능이 포함되어 있습니다.

### 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.

**Command Injection:**

Out-of-band Application Security Testing(OAST) 기능[3].을 지원하는 페이로드를 사용할 수 있도록 ID 11722 및 11723으로 식별되는 검사가 추가되었습니다. 이러한 검사를 실행하면 오탐지를 줄이고 WebInspect 검사 결과의 정확도를 높일 수 있습니다.

# Fortify Premium Content

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

### OWASP MASVS v2.0.0

이번 릴리스에는 상기 언급했던 것처럼 OWASP MASVS v2.0.0 버전과 연관된 Fortify의 분류가 추가되었을 뿐 아니라, OWASP MASVS v2.0.0을 지원하는 Fortify Software Security Center용 신규 보고서 번들도 포함되었습니다. Fortify 고객 지원 포털의 Premium Content에서 해당 번들을 다운로드할 수 있습니다.

[3] 11723 검사는 많은 수의 요청을 전송하므로 표준 정책에서는 제외되었습니다. 모두 검사 정책을 사용하거나 검사를 포함하도록 기존 정책을 사용자 지정하거나 이 검사를 실행하는 사용자 지정 정책을 만드십시오.

**Fortify Taxonomy: 소프트웨어 보안 오류**

Fortify Taxonomy 사이트(https://vulncat.fortify.com)에는 새로 추가된 범주 지원에 대한 설명이 수록되어 있습니다.
이제 고객은 상기 라이브 사이트와 일치하는 Fortify Taxonomy 사이트의 새로운 오프클라우드 버전도 Fortify 지원 포털에서 다운로드할 수 있습니다.

## Fortify 기술 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