Fortify 소프트웨어 보안 콘텐츠

2023 업데이트 3
2023년 9월 29일 금요일

OpenText 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 33개 이상의 프로그래밍 언어에서 1,627개의 취약점 범주를 지원하며 적용되는 개별 API는 1백만 개가 넘습니다.

Fortify Software Security Research (SSR) 팀은 Fortify Secure Coding Rulepacks(영어, 버전 2023.3.0), 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]

이 릴리스에서 Fortify Secure Coding Rulepacks는 33개 이상의 프로그래밍 언어에서 1,403가지 고유 범주의 취약점을 감지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Android 13에 대한 지원 개선(지원되는 버전: 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. 이번 릴리스에는 Android 응용 프로그램용으로 다음의 3가지 신규 취약성 범주가 추가되었습니다.

- Intent Manipulation: Implicit Internal Intent
- Intent Manipulation: Implicit Pending Intent
- Intent Manipulation: Mutable Pending Intent

Android Jetpack(AndroidX) 최초 지원

Android Jetpack은 개발자가 Android 응용 프로그램을 더욱 쉽게 만드는 데 도움이 되는 라이브러리, 도구 및 지침 세트입니다. Jetpack은 androidx.* 패키지를 포함하며, 플랫폼 API에서 번들로 제공되지 않으므로 이전 버전과의 호환이 가능하고 보다 자주 업데이트할 수 있습니다. 이번 릴리스에서는 이 소프트웨어 제품군에 대한 최초 지원 범위를 제공합니다.

Android Jetpack의 최초 지원 범위는 다음 라이브러리의 취약성 감지를 지원합니다.

- androidx.appsearch (version supported: 1.1.0-alpha03)
- androidx.compose.foundation (version supported: 1.5.1)
- androidx.compose.material (version supported: 1.5.1)
- androidx.compose.material3 (version supported: 1.1.2)
- androidx.compose.ui (version supported: 1.5.1)
- androidx.core (version supported: 1.12.0)
- androidx.credentials (version supported: 1.2.0-beta04)
- androidx.datastore (version supported: 1.0.0)
- androidx.security.crypto (version supported: 1.0.0)
- androidx.sqlite (version supported: 2.3.1)

향상된 범주 지원 범위의 예는 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

MySQL Connector/Python 지원(지원되는 버전: 8.1.0)

MySQL Connector/Python은 Python 응용 프로그램과 MySQL 데이터베이스 간의 상호 작용을 가능하게 하는 소프트웨어 라이브러리입니다. 이는 Python 프로그래밍 언어와 MySQL 데이터베이스 관리 시스템 간의 브리지 또는 커넥터 역할을 하여 개발자가 Python 코드를 사용하여 MySQL 데이터베이스의 데이터를 손쉽게 연결, 쿼리 및 조작할 수 있도록 합니다.

향상된 범주 지원 범위에는 다음이 포함됩니다.

- Access Control: Database
- Denial of Service
- Insecure Transport: Client Identity Verification Disabled
- Insecure Transport: Database
- Insecure Transport: Weak SSL Protocol
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Path Manipulation
- Server-Side Request Forgery
- SQL Injection

Django에 대한 지원 개선(지원되는 버전: 3.2)

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 범위를 업데이트하여 최대 버전 3.2까지의 릴리스를 지원합니다.

향상된 지원 범위에는 다음 네임스페이스가 포함됩니다. *Django.contrib.auth.models, Django.db.models* 및 *Django.http.response*. 또한 취약성 범주에 대한 향상된 지원 범위에는 다음이 포함됩니다.

- Cookie Security: Overly Permissive SameSite Attribute
- Header Manipulation
- Password Management

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- System Information Leak
- System Information Leak: External

Bicep 최초 지원(지원되는 버전: 0.21.1)[1]

Microsoft Bicep은 Azure 리소스 배포를 단순화하고 간소화하기 위해 Microsoft에서 개발한 IaC(코드형 인프라) 솔루션용 오픈 소스 DSL(도메인별 언어)입니다. 이는 ARM(Azure Resource Manager) 템플릿 위에서 추상화 계층 역할을 하여 Azure 인프라를 정의하고 관리하기 위해 보다 직관적이고 읽기 쉬운 방법을 제공합니다. Bicep을 사용하면 사용자는 간결하고 사람이 읽을 수 있는 코드를 작성하여 Azure 리소스, 구성 및 종속성을 설명할 수 있습니다.

취약성 범주의 최초 지원 범위에는 다음이 포함됩니다.

- Azure ARM Misconfiguration: Automation Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Batch Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Cognitive Services Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Databricks Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Event Hubs Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Hardcoded Secret
- Azure ARM Misconfiguration: HTTPS Not Required
- Azure ARM Misconfiguration: Improper AKS Network Access Control
- Azure ARM Misconfiguration: Improper App Service Access Control
- Azure ARM Misconfiguration: Improper Blob Storage Access Control
- Azure ARM Misconfiguration: Improper Compute VM Access Control
- Azure ARM Misconfiguration: Improper Container Registry Network Access Control
- Azure ARM Misconfiguration: Improper CORS Policy
- Azure ARM Misconfiguration: Improper Custom Role Access Control Policy
- Azure ARM Misconfiguration: Improper DocumentDB Network Access Control
- Azure ARM Misconfiguration: Improper KeyVault Access Control Policy
- Azure ARM Misconfiguration: Improper Security Group Network Access Control
- Azure ARM Misconfiguration: Improper SQL Server Network Access Control
- Azure ARM Misconfiguration: Improper Storage Network Access Control
- Azure ARM Misconfiguration: Insecure Active Directory Domain Service Transport
- Azure ARM Misconfiguration: Insecure App Service Transport
- Azure ARM Misconfiguration: Insecure CDN Transport
- Azure ARM Misconfiguration: Insecure Database for MySQL Storage
- Azure ARM Misconfiguration: Insecure Database for PostgreSQL Storage
- Azure ARM Misconfiguration: Insecure DataBricks Storage
- Azure ARM Misconfiguration: Insecure EventHub Storage
- Azure ARM Misconfiguration: Insecure EventHub Transport
- Azure ARM Misconfiguration: Insecure IoT Hub Transport
- Azure ARM Misconfiguration: Insecure MySQL Server Transport
- Azure ARM Misconfiguration: Insecure PostgreSQL Server Transport

[1] Fortify Static Code Analyzer 23.2.0 이상이 필요합니다. Bicep의 최초 보안 콘텐츠는 Fortify Static Code Analyzer 23.2.x로 배포됩니다.

- Azure ARM Misconfiguration: Insecure Recovery Services Backup Storage
- Azure ARM Misconfiguration: Insecure Recovery Services Vaults Storage
- Azure ARM Misconfiguration: Insecure Redis Enterprise Transport
- Azure ARM Misconfiguration: Insecure Redis Transport
- Azure ARM Misconfiguration: Insecure Service Bus Storage
- Azure ARM Misconfiguration: Insecure Service Bus Transport
- Azure ARM Misconfiguration: Insecure Storage Account Storage
- Azure ARM Misconfiguration: Insecure Storage Account Transport
- Azure ARM Misconfiguration: Insufficient AKS Monitoring
- Azure ARM Misconfiguration: Insufficient Application Insights Logging
- Azure ARM Misconfiguration: Insufficient Application Insights Monitoring
- Azure ARM Misconfiguration: Insufficient Microsoft Defender Monitoring
- Azure ARM Misconfiguration: Insufficient SQL Server Logging
- Azure ARM Misconfiguration: Insufficient SQL Server Monitoring
- Azure ARM Misconfiguration: IoT Hub Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: NetApp Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Public Access Allowed
- Azure ARM Misconfiguration: Service Bus Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Storage Account Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Weak App Service Authentication
- Azure ARM Misconfiguration: Weak SignalR Authentication
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Privacy Violation
- Privacy Violation: Missing Secure Decorator

Solidity 최초 지원(지원되는 버전: 0.8.x)[2]

Solidity는 다양한 분산형 블록체인 환경, 특히 이더리움 블록체인에서 스마트 계약을 개발하는 데 사용되는 객체 지향 프로그래밍 언어입니다. Solidity로 작성된 스마트 계약은 주로 EVM(Ethereum Virtual Machine)에서 실행되지만 다른 호환 가능한 가상 머신에서도 실행될 수 있습니다.

취약성 범주의 최초 지원 범위에는 다음이 포함됩니다.

- Authorization Bypass: tx.origin
- Code Correctness: Failing Assertion
- Code Correctness: Reentrancy
- Code Correctness: Typographical Error
- Dead Code
- Denial of Service: External Call
- Dynamic Code Evaluation: Delegatecall
- Integer Overflow
- Obsolete
- Often Misused: Block Values
- Poor Style: Confusing Naming

[2] Fortify Static Code Analyzer 23.2.0 이상이 필요합니다. Solidty의 최초 보안 콘텐츠는 Fortify Static Code Analyzer 23.2.x로 배포됩니다.

- Poor Style: Variable Never Used
- Solidity Bad Practices: Default Function Visibility
- Solidity Bad Practices: Ether Balance Check
- Solidity Bad Practices: Hardcoded Gas Amount
- Solidity Bad Practices: Lack of Explicit Variable Visibility
- Solidity Bad Practices: Missing Constructor
- Solidity Misconfiguration: Compiler With Known Vulnerabilities
- Solidity Misconfiguration: Floating Pragma
- Unchecked Return Value
- Uninitialized Variable

클라우드 IaC(코드형 인프라)

IaC(코드형 인프라)는 다양한 수동 프로세스가 아닌 코드를 통해 컴퓨터 리소스를 관리하고 프로비저닝하는 프로세스입니다. 이번 릴리스에서는 지원되는 기술의 범위가 확장되어 Microsoft Azure 배포용 Terraform 구성 및 AWS Ansible용 구성이 모두 지원됩니다. 그리고 이러한 서비스의 구성과 관련된 일반적인 문제가 이제 개발자에게 보고됩니다.

Microsoft Azure 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 Microsoft Azure 인프라의 구성 및 관리를 지원합니다. Terraform 구성에 대한 향상된 취약성 범주 지원 범위에는 다음이 포함됩니다.

- Azure Terraform Misconfiguration: App Service Auto Upgrade Disabled
- Azure Terraform Misconfiguration: Improper AKS Access Control
- Azure Terraform Misconfiguration: Improper AKS Network Access Control
- Azure Terraform Misconfiguration: Improper App Service Access Control
- Azure Terraform Misconfiguration: Improper Cognitive Search Network Access Control
- Azure Terraform Misconfiguration: Improper Container Registry Access Control
- Azure Terraform Misconfiguration: Improper Functions Access Control
- Azure Terraform Misconfiguration: Improper MariaDB Network Access Control
- Azure Terraform Misconfiguration: Improper MySQL Network Access Control
- Azure Terraform Misconfiguration: Improper SQL Database Network Access Control
- Azure Terraform Misconfiguration: Improper Storage Account Access Control
- Azure Terraform Misconfiguration: Improper Virtual Network Access Control
- Azure Terraform Misconfiguration: Insecure Disk Storage
- Azure Terraform Misconfiguration: Insecure PostgreSQL Storage
- Azure Terraform Misconfiguration: Insufficient AKS Monitoring
- Azure Terraform Misconfiguration: Insufficient Application Gateway Monitoring
- Azure Terraform Misconfiguration: Insufficient Defender for Cloud Monitoring
- Azure Terraform Misconfiguration: Insufficient Front Door Monitoring
- Azure Terraform Misconfiguration: Insufficient MariaDB Backup
- Azure Terraform Misconfiguration: Insufficient Monitor Logging
- Azure Terraform Misconfiguration: Insufficient Network Watcher Logging
- Azure Terraform Misconfiguration: Insufficient PostgreSQL Monitoring
- Azure Terraform Misconfiguration: Insufficient SQL Database Monitoring
- Azure Terraform Misconfiguration: Redis Cache Auto Upgrade Disabled

- Azure Terraform Misconfiguration: Reduced Virtual Network Availability
- Azure Terraform Misconfiguration: Weak App Service Authentication
- Azure Terraform Misconfiguration: Weak Functions Authentication
- Azure Terraform Misconfiguration: Weak Linux Virtual Machines Authentication
- Azure Terraform Misconfiguration: Weak Service Fabric Authentication

Amazon Web Services(AWS) Ansible 구성

Ansible은 구성 관리, 응용 프로그램 배포, 클라우드 프로비저닝, 다양한 환경으로 노드 오케스트레이션과 같은 기능을 제공하는 오픈 소스 자동화 기능입니다. Ansible에는Amazon Web Services(AWS)의 구성 및 관리를 지원하는 모듈이 포함되어 있습니다. AWS Ansible 구성에 대한 향상된 취약성 범주 지원 범위에는 다음이 포함됩니다.

- AWS Ansible Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS Ansible Misconfiguration: Improper API Gateway Network Access Control
- AWS Ansible Misconfiguration: Improper ECR Access Control
- AWS Ansible Misconfiguration: Improper ECS Network Access Control
- AWS Ansible Misconfiguration: Improper S3 Access Control
- AWS Ansible Misconfiguration: Improper Stack Access Control
- AWS Ansible Misconfiguration: Insecure API Gateway Transport
- AWS Ansible Misconfiguration: Insecure CloudFront Transport
- AWS Ansible Misconfiguration: Insecure CloudTrail Storage
- AWS Ansible Misconfiguration: Insecure CodeBuild Storage
- AWS Ansible Misconfiguration: Insecure RDS Transport
- AWS Ansible Misconfiguration: Insufficient API Gateway Logging
- AWS Ansible Misconfiguration: Insufficient CloudFront Logging
- AWS Ansible Misconfiguration: Insufficient Lambda Logging
- AWS Ansible Misconfiguration: Insufficient RDS Backup
- AWS Ansible Misconfiguration: Insufficient S3 Backup
- AWS Ansible Misconfiguration: Insufficient S3 Logging
- AWS Ansible Misconfiguration: Insufficient S3 Monitoring
- AWS Ansible Misconfiguration: Insufficient Stack Monitoring
- AWS Ansible Misconfiguration: Privileged Batch Container
- AWS Ansible Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Ansible Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS Ansible Misconfiguration: Reduced CloudFront Availability
- AWS Ansible Misconfiguration: Reduced EC2 Availability
- AWS Ansible Misconfiguration: Reduced ELB Availability
- AWS Ansible Misconfiguration: Weak IAM Password Policy

2023 CWE™(Common Weakness Enumeration) Top 25

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Weaknesses(CWE Top 25)는 2019년에 도입되었으며 SANS Top 25를 대체합니다. 2023년 6월에 릴리스된 2023 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 취약점을 중심으로 감사의 우선 순위를 지정하고자 하는 고객을 지원하기 위해, Fortify Taxonomy와 2023 CWE Top 25 사이의 상관 관계가 추가되었습니다.

OWASP API Security Top 10 2023

OWASP(Open Worldwide Application Security Project) API Security Top 10 2023에서는 2023년 API에 영향을 미치는 주요 보안 위험 목록을 제공합니다. 이는 API 보안 취약점에 대한 인식을 높이고 웹 API를 보호해야 하는 개발자, 디자이너, 설계자, 관리자 및/또는 일반적인 조직과 같이 API 개발 및 유지 관리에 관련된 사람들을 교육하는 것을 목표로 합니다.

OWASP API Security Top 10은 웹 API에 영향을 미치는 취약점에 중점을 두고 있습니다. 이는 단독으로 사용하기 위한 것이 아닌, 모든 관련 위험을 철저히 잡아내기 위해 다른 표준 및 모범 사례와 결합하여 사용하기 위해 고안되었습니다. 예를 들어 주입과 같은 입력 검증과 관련된 문제를 식별하려면 OWASP Top 10과 결합하여 사용해야 합니다. 웹 응용 프로그램 위험을 경감하고자 하는 고객을 지원하기 위해 새롭게 릴리스된 OWASP API Security Top 10 2023과 연관된 Fortify Taxonomy가 추가되었습니다.

CIS(Center for Internet Security) 벤치마크

CIS(Center for Internet Security) 벤치마크는 CIS 중요 보안 제어에 매핑되는 커뮤니티에서 개발한 보안 구성 권장 사항 모음입니다. 이러한 권장 사항은 클라우드 인프라를 보호하고 업계 표준으로 컴플라이언스를 입증하기 위한 것입니다. CIS 벤치마크는 25개 이상의 적용되는 공급업체 제품군에 대한 사이버 보안의 진화하는 상태에 적응하기 위해 지속적으로 업데이트됩니다. 지원되는 제품군은 다음과 같습니다.

- Amazon Elastic Kubernetes Service(EKS) Benchmark v1.3.0
- Amazon Web Services Foundations Benchmark v2.0.0
- Azure Kubernetes Service(AKS) Benchmark v1.3.0
- Google Cloud Computing Platform Benchmark v2.0.0
- Google Kubernetes Engine(GKE) Benchmark v1.4.0
- Kubernetes Benchmark v1.7.1
- Microsoft Azure Foundations Benchmark v2.0.0

SWC(Smart Contract Weakness Classification)[3]

SWC(Smart Contract Weakness Classification)는 스마트 계약의 취약점을 분류하고 설명하는 체계적인 프레임워크입니다. 이더리움과 같은 블록체인에서 실행되는 자체 실행 코드 조각의 취약점을 이해하고 해결하는 표준화된 방법을 제공합니다. 특히, SWC 레지스트리의 컨텐츠는 2020년 이후 포괄적으로 업데이트되지 않아 알려진 불완전성, 오류 및 중요한 누락 등의 결과를 낳았습니다. 스마트 계약의 위험을 경감하고자 하는 고객을 위해 현재 SWC 버전과 연관된 Fortify Taxonomy가 추가되었습니다.

[3] Fortify Static Code Analyser 23.2.0 이상에서의 스캔이 필요합니다.

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

2022.4 릴리스에서 관찰된 바와 같이 Fortify Static Code Analyzer의 마지막 4개 주 릴리스는 계속됩니다. 따라서 이번 릴리스는 20.x 이전 Fortify Static Code Analyzer 버전을 지원하는 Rulepacks의 마지막 릴리스입니다. 다음 릴리스에서는 20.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.

오탐지 개선 사항

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

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* – ASP.NET 응용 프로그램에서 가상 필드와 관련된 오탐지가 제거됨
- *Code Correctness: Double-Checked Locking* – Java 응용 프로그램에서 오탐지가 제거됨
- *Cross-Site Request Forgery* – NET 응용 프로그램에서 `AntiForgery.GetHtml()` 또는 `Html.AntiForgeryToken()`을 사용하는 HTML 양식에 대한 오탐지가 제거됨
- *Cross-Site Scripting: Persistent* – Django 응용 프로그램에서 `cycle` 태그와 관련된 오탐지 제거
- *Double Free* – 성능 향상 라이브러리의 `throw_error()`를 사용하는 C/C++ 응용 프로그램에서 오탐지 제거가 제거됨
- *HTML5: Missing Content Security Policy* – Java 응용 프로그램에서 오탐지가 제거됨
- *JSON Injection* – PHP 응용 프로그램에서 오탐지가 제거됨
- *Mass Assignment: Insecure Binder Configuration* – .NET 응용 프로그램에서 Enum 유형과 관련된 오탐지가 제거됨
- *Often Misused: File System* – C++ 응용 프로그램에서 `GetFullPathNameW()` 및 유사한 함수 호출과 관련된 오탐지가 제거됨
- *Path Manipulation* – Amazon AWS SDK를 사용하는 Java 응용 프로그램에서 오탐지가 제거됨
- *Type Mismatch: Signed to Unsigned* – C/C++ 응용 프로그램에서 부울 값과 관련된 오탐지가 제거됨
- *Unreleased Resource* – C++ 응용 프로그램에서 `CreateFileW()`를 사용할 때 오탐지가 제거됨

범주 변경

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

일관성을 개선하기 위해 다음 14개 범주의 이름이 변경되었습니다.

제거된 범주	추가된 범주
AWS CloudFormation Misconfiguration: Insecure Elasticache Storage	AWS CloudFormation Misconfiguration: Insecure ElastiCache Storage
AWS CloudFormation Misconfiguration: Insecure Elasticache Transport	AWS CloudFormation Misconfiguration: Insecure ElastiCache Transport
AWS Terraform Misconfiguration: Elasticache Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
Azure Terraform Bad Practices: AKS Cluster Missing Host-Based Encryption	Azure Terraform Misconfiguration: AKS Cluster Missing Host-Based Encryption
Azure Terraform Bad Practices: Azure MySQL Server Missing Infrastructure Encryption	Azure Terraform Misconfiguration: MySQL Missing Infrastructure Encryption
Azure Terraform Bad Practices: Azure PostgreSQL Server Missing Infrastructure Encryption	Azure Terraform Misconfiguration: PostgreSQL Missing Infrastructure Encryption
Azure Terraform Bad Practices: Missing Azure Storage Infrastructure Encryption	Azure Terraform Misconfiguration: Storage Account Missing Infrastructure Encryption
Azure Terraform Bad Practices: Missing SQL Database Backup Encryption	Azure Terraform Misconfiguration: SQL Server Backup Missing Encryption
Azure Terraform Bad Practices: Scale Set Missing Host-Based Encryption	Azure Terraform Misconfiguration: Scale Set Missing Host-Based Encryption
Azure Terraform Bad Practices: VM Missing Host-Based Encryption	Azure Terraform Misconfiguration: VM Missing Host-Based Encryption
GCP Terraform Bad Practices: Overly Permissive Service Account	GCP Terraform Misconfiguration: Improper Compute Engine Access Control
GCP Terraform Misconfiguration: Weak Key Management	GCP Terraform Misconfiguration: Compute Engine Missing Customer-Managed Encryption Key
Kubernetes Bad Practices: Improper Admission Controller Access Control	Kubernetes Misconfiguration: Improper Admission Controller Access Control
Kubernetes Misconfiguration: Missing Service Account Admission Controller	Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller

Fortify 우선 순위 변경

누락된 고객 관리 암호화 키와 관련된 취약성 범주 전체의 일관성을 개선하기 위해 다음 20개 범주의 Fortify 우선 순위가 "낮음"으로 변경되었습니다.

- *Azure ARM Misconfiguration: Automation Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Batch Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Cognitive Services Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Databricks Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Event Hubs Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: IoT Hub Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: NetApp Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Service Bus Missing Customer-Managed Encryption Key*

- *Azure ARM Misconfiguration: Storage Account Missing Customer-Managed Encryption Key*
- *Azure Terraform Misconfiguration: AKS Cluster Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Azure Disk Snapshot Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Container Registry Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Cosmos DB Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Managed Disk Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Shared Image Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: SQL Database Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Storage Account Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Storage Encryption Scope Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: VM Storage Missing Customer-Managed Key*
- *GCP Terraform Misconfiguration: Compute Engine Missing Customer-Managed Encryption Key*

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

vBulletin 버전 5.6.0-5.6.8의 사전 RCE(Remote Code Execution) 취약점이 CVE-2023-25135에 의해 식별되었습니다. 동적 온라인 커뮤니티 및 포럼을 구축하는 데 널리 사용되는 소프트웨어인 vBulletin은 인증되지 않은 역직렬화를 위해 사용자가 제공한 입력을 부적절하게 제거합니다. 이 문제로 인해 공격자는 서버에서 임의의 코드를 실행하거나 응용 프로그램 논리를 남용하거나 서비스 거부(DoS) 공격을 시작할 수 있습니다. 이번 릴리스에는 대상 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

프로토타입 오염: 서버 측

서버 측 프로토타입 오염은 공격자가 객체의 프로토타입을 조작할 수 있을 때 발생합니다. 이는 런타임에서 속성과 메서드를 변경할 수 있는 JavaScript와 같은 프로토타입 기반 언어에서 가능합니다. 악용의 심각도는 오염된 객체가 응용 프로그램에서 사용되는 위치에 따라 달라집니다. 공격에는 서비스 거부, 응용 프로그램 구성 변경 및 경우에 따라 Remote Code Execution이 포함됩니다. 이 릴리스에는 웹 응용 프로그램에서 프로토타입 오염을 감지하는 검사 기능이 포함되어 있습니다.

컴플라이언스 보고서

2023 CWE™(Common Weakness Enumeration) Top 25

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Weaknesses(CWE Top 25)는 2019년에 도입되었으며 SANS Top 25를 대체합니다. 6월에 릴리스된 2023 CWE Top 25는 지난 2년 동안 NVD(National Vulnerability Database)에 보고된 취약성의 빈도 및 심각도를 정규화하는 추론적 공식을 사용하여 결정되었습니다. 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.

OWASP API Security Top 10 2023

OWASP(Open Worldwide Application Security Project) API Security Top 10 2023에서는 2023년 API에 영향을 미치는 주요 보안 위험 목록을 제공합니다. 이는 API 보안 취약점에 대한 인식을 높이고 웹 API를 보호해야 하는 개발자, 디자이너, 설계자, 관리자 및 일반적인 조직과 같이 API 개발 및 유지 관리에 관련된 사람들을 교육하는 것을 목표로 합니다. OWASP API Security Top 10은 웹 API에 영향을 미치는 취약점에 중점을 두고 있습니다. 이는 단독으로 사용하기 위한 것이 아닌, 모든 관련 위험을 철저하게 잡아내기 위해 다른 표준 및 모범 사례와 결합하여 사용하도록 고안되었습니다. 예: OWASP API Security Top 10 2023을 OWASP Top 10과 결합하여 주입과 같은 입력 검증과 관련된 문제를 식별할 수 있습니다. 이 SecureBase 업데이트에는 OWASP API Security Top 10 2023 범주와 WebInspect 검사 간의 연관성을 제공하는 새로운 컴플라이언스 보고서 템플릿이 포함됩니다.

정책 업데이트

2023 CWE Top 25

2023 CWE Top 25 관련 검사를 포함하도록 사용자 지정된 정책이 WebInspect SecureBase의 지원되는 정책 목록에 추가되었습니다.

OWASP API Security Top 10 2023

OWASP API Security Top 10 2023 관련 검사를 포함하도록 사용자 지정된 정책이 WebInspect SecureBase의 지원되는 정책 목록에 추가되었습니다. 이 정책에는 고객이 컴플라이언스별 WebInspect 검사를 실행할 수 있도록 하는 사용 가능한 WebInspect 검사의 하위 집합이 포함됩니다.

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.

LDAP Injection

이 릴리스에는 오탐지를 줄이고 결과의 정확성을 높이기 위한 LDAP 주입 검사 개선 사항이 포함되어 있습니다.

SSL 인증서 호스트 이름 불일치

이제 SSL 인증서 호스트 이름 불일치 확인 보고서 내용에는 고객이 이 보안 문제에 대한 수정 사항을 적절하게 적용하는 데 도움이 되는 더 자세한 정보가 포함됩니다.

적극적인 적용 범위를 사용하는 검사 입력

일부 WebInspect 검사의 경우 WebInspect가 더 넓은 범위의 엔드포인트를 대상으로 하는 더 긴 공격 목록을 보내도록 하는 적극적인 적용 범위를 활성화할 수 있습니다. 이 릴리스에는 고객이 스캔 정책에 별도의 검사를 추가하는 대신 검사 입력을 변경하여 적극적인 적용 범위를 구성할 수 있는 등의 개선 사항이 포함되어 있습니다. 적극적인 적용 범위 기능이 있는 검사에는 다음이 포함됩니다. *Log4Shell*, *JNDI Reference Injection*, *Server-Side Request Forgery*, *OS Command Injection* 및 *Server-Side Prototype Pollution*. 적극적인 적용 범위를 사용하는 검사를 활성화하면 보다 정확한 검사를 제공하지만 요청 수와 검사 시간이 급격히 증가할 수 있다는 점을 고려해야 합니다. 따라서 Fortify에서는 다른 검사 없이 별도의 정책에서 적극적인 적용 범위를 사용하는 검사 기능을 활성화하여 실행할 것을 강력히 권장합니다.

웹 서버 구성 오류: 보호되지 않은 파일

이 릴리스에는 Java 관련 구성 파일 감지 기능을 개선하기 위한 사소한 버그 수정이 포함되어 있습니다.

Fortify Premium Content

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

2023 CWE Top 25

새로운 상관 관계를 뒷받침하기 위해 이 릴리스에는 2023 CWE Top 25를 지원하는 Fortify Software Security Center에 대한 새로운 보고서 번들이 포함되어 있으며 Fortify 고객 지원 포털의 Premium Content에서 다운로드할 수 있습니다.

OWASP API Security Top 10 2023

새로운 상관 관계를 뒷받침하기 위해 이 릴리스에는 OWASP API Security Top 10을 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.

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