Fortify 소프트웨어 보안 콘텐츠

2024 업데이트 2
2024년 6월 28일 금요일

OpenText Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구를 OpenText™ Fortify Static Code Analyzer 및 OpenText™ Fortify WebInspect를 포함한 Fortify 제품 포트폴리오를 강화하는 보안 인텔리전스로 변환하는 일을 하고 있습니다. 현재 Fortify 소프트웨어 보안 컨텐츠는 33개 이상의 프로그래밍 언어에서 1,660개의 취약점 범주를 지원하며 적용되는 개별 API는 1백만 개가 넘습니다.

Fortify Software Security Research (SSR) 팀은 Fortify Secure Coding Rulepacks(영어, 버전 2024.2.0), 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 33개 이상의 프로그래밍 언어에서 1,435가지 고유 범주의 취약점을 감지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Node.js에 대한 지원 개선(지원되는 버전: 21.x)[1]

Node.js는 개발자가 서버, 웹 응용 프로그램, 명령줄 도구 등을 만들 수 있는 크로스 플랫폼 JavaScript 런타임 환경입니다. 이 릴리스에는 Node.js 21.x의 다음 모듈에 대한 Node.js 지원 관련 중요한 업데이트가 포함되어 있습니다.

- async_hooks
- buffer
- child_process
- crypto
- dgram
- dns
- fs
- http
- https
- net
- os
- path
- process
- punycode
- querystring
- stream
- string_decoder
- timers
- tls
- url
- util
- v8
- vm
- worker_threads
- zlib

이러한 업데이트를 설치하면 다음과 같은 취약성 범주에서 문제를 더욱 정확하게 감지할 수 있습니다.

- Command Injection
- Dynamic Code Evaluation: Code Injection
- Header Manipulation

[1] Fortify Static Code Analyzer 24.2 이상이 필요합니다.

- Insecure Transport: Weak SSL Cipher
- Insecure Transport: Weak SSL Protocol
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- System Information Leak: External

또한 이번 릴리스에는 Android 응용 프로그램용으로 다음의 취약성 범주가 추가되었습니다.

- DNS Spoofing
- Dynamic Code Evaluation: Script Injection
- Insecure Transport: Insufficient Diffie Hellman Strength
- Key Management: Empty HMAC Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- 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: Predictable Salt
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Stream Cipher

Java에 대한 지원 개선(지원되는 버전: 21)

Java 21은 Java 플랫폼을 위한 최신 LTS(장기 지원) 버전입니다. 여기에는 기존 API에 대한 개선 사항이 포함되어 있지만 다수의 신규 기능도 포함되어 있습니다. 가장 중요한 기능 중 일부는 다음과 같습니다. 외부 함수 및 메모리, 시퀀스 컬렉션, 키 캡슐화, 가상 스레드, 구조화된 동시성, 이름 없는 변수 및 범위가 지정된 값. 이러한 기능 중 일부는 아직 미리 보기 상태이지만 적용 범위를 포함할 만큼 성숙도가 높은 것으로 간주됩니다. 업데이트된 범주는 다음과 같습니다.

- Process Control
- Unreleased Resource
- Weak Encryption
- Weak Cryptographic Hash

또한 다음과 같은 새로운 범주가 지원됩니다.

- Restricted Method
- Weak Cryptographic Signature: XML Signature Secure Validation Disabled

MyBatis에 대한 지원 개선(지원되는 버전: 3.5.x)

MyBatis는 관계형 데이터베이스의 개체를 개체 지향 응용 프로그램의 개체와 연결하는 데 사용되는 SQL 매퍼입니다. 이 프레임워크는 XML 설명자 또는 코드 주석을 사용하여 저장 프로시저 및 SQL 문을 페어링하여 개발 프로세스와 데이터베이스 통신을 용이하게 합니다. MyBatis에 대한 지원이 버전 3.5.16으로 향상되었습니다. 개선 사항에는 다음의 취약성 범주에 대한 업데이트된 지원이 포함됩니다.

- Dynamic Code Evaluation: Unsafe Deserialization
- SQL Injection
- System Information Leak
- Unreleased Resource: Database
- Unsafe Reflection

MyBatis-Plus 최초 지원(지원되는 버전: 3.5.x)

MyBatis-Plus는 원래 프레임워크에서 확인할 수 있는 것 이상으로 유용하고 효율적인 기본 기능을 제공함으로써 개발을 간소화하기 위해 기존 MyBatis 프레임워크를 기반으로 구축되었습니다. MyBatis - Plus 3.5.x에 대한 최초 지원이 제공됩니다. *SQL Injection*에 대한 최초 범주 지원이 제공됩니다.

AI(인공 지능) 및 ML(기계 학습) 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. 이번 릴리스에서는 OpenAI API(Python 및 JavaScript), TensorFlow(Python) 또는 Anthropic Claude(Python 및 JavaScript)를 사용하는 프로젝트에 대한 적용 범위가 개선됩니다. Fortify는 지원 대상 프로젝트에서 AI/ML 모델 API가 전송하는 응답의 암시적 신뢰로 인해 발생하는 취약성을 감지하며 다음과 같은 기능도 제공합니다.

OpenAI에 대한 지원 개선(지원되는 버전: 1.14.x[Python], 4.33.x[JavaScript])

Python, TypeScript 및 JavaScript용 OpenAI 라이브러리는 고급 AI 기능을 다양한 응용 프로그램에 통합하기 위한 포괄적인 도구를 제공합니다. 이러한 라이브러리는 자연어 처리, 텍스트 생성, 대화형 AI를 비롯한 다양한 기능을 지원합니다. 개발자는 직관적이고 사용자에게 친숙한 API를 통해 OpenAI의 최첨단 AI 모델을 프로젝트에 원활하게 포함할 수 있어 Python, TypeScript 및 JavaScript 환경 전반에서 상호 작용 및 인텔리전스가 향상됩니다. 이번 개선된 지원에서는 *Cross-Site Scripting: AI*에 대한 적용 범위가 확장되며, 다음의 두 가지 신규 취약성 범주가 추가됩니다.

- Cross-Site Scripting: DOM AI
- Prompt Injection

TensorFlow(지원되는 버전: 2.16.x)

Google의 선도적인 오픈소스 기계 학습 프레임워크인 TensorFlow는 기계 학습 모델을 만들고 배포하기 위한 강력한 도구 모음을 제공합니다. 내장된 라이브러리와 사전 훈련된 모델을 통해 딥 러닝 응용 프로그램 구축을 간소화합니다. TensorFlow는 연구 프로토타입부터 대규모 프로덕션 시스템에 이르기까지 다양한 프로젝트 컬렉션에 맞게 확장 가능합니다. 최초 적용 범위에는 다음 범주에 대한 지원이 포함됩니다.

- Path Manipulation
- Privacy Violation
- System Information Leak: Internal

또한 지원에는 다음의 신규 취약성 범주가 추가됩니다.

- Dynamic Code Evaluation: Unsafe TensorFlow Deserialization

Anthropic Claude SDK(지원되는 버전: 0.21.3[Python], 0.20.5[JavaScript])

Python 및 JavaScript용 Anthropic Claude 라이브러리는 정교한 AI 언어 모델인 Claude를 응용 프로그램에 통합하기 위한 포괄적인 도구를 제공합니다. 최초 적용 범위에는 *Cross-Site Scripting: AI*에 대한 지원이 포함되어 있으며, 다음의 두 가지 신규 취약성 범주가 추가됩니다.

- Cross-Site Scripting: DOM AI
- Prompt Injection

Django에 대한 지원 개선(지원되는 버전: 5.0.x)

Django는 안전하고 신속한 웹 개발을 할 수 있도록 설계되어 왔으며 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 적용 범위를 업데이트하여 최대 버전 5.0.x까지의 릴리스를 지원합니다.

이러한 업데이트를 설치하면 다음과 같은 취약성 범주에서 문제를 더욱 정확하게 감지할 수 있습니다.

- Access Control: Database
- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Cross-Frame Scripting
- Cross-Site Request Forgery
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Transport
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Privacy Violation: BREACH
- SQL Injection

Paramiko 최초 지원(지원되는 버전: 3.4.x)

Paramiko는 SSH를 통해 컴퓨터에 연결하기 위한 Python 라이브러리입니다. Paramiko는 개발자로부터 암호화 메서드를 추상화하는 기능 도구 모음을 제공합니다. 이는 소켓 프로그래밍과 유사한 높은 수준의 기능을 제공하고, 개발자에게 SSH 연결의 세부 관리 구성을 위한 하위 수준의 방법에 대한 액세스 권한을 부여합니다. 최초 지원에는 다음과 같은 취약성 범주가 포함됩니다.

- Command Injection
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Cipher
- Password Management: Hardcoded Password
- SSH Misconfiguration: Missing Authentication

PHP에 대한 지원 개선(지원되는 버전: 8.3)

PHP는 웹 개발에 가장 자주 사용되고 널리 사용되는 범용 스크립팅 언어입니다. 이번 릴리스 업데이트는 PHP 버전 8.3까지 지원합니다. 구체적으로 이번 릴리스에는 다음과 같은 확장에 대한 개선된 지원이 포함됩니다.

- DOM(지원되는 버전: 8.3)

  PHP의 DOM 확장을 통해 문서 개체 모델을 사용하여 PHP에서 XML 및 HTML 문서에 대한 작업을 수행할 수 있습니다. 이 라이브러리에 대한 확장된 지원에는 DOM 작업에 대한 향상된 데이터 흐름 지원과 *Setting Manipulation* 취약성 식별을 위한 추가 적용 범위가 포함됩니다.

- JSON(지원되는 버전: 8.3)

  PHP의 JSON 확장을 통해 PHP 라이센스에 따라 작성되고 라이센스가 부여된 JSON 구문 분석기를 사용할 수 있습니다. 이 확장에 대한 최초 지원에는 확장 기능에 대한 데이터 흐름 지원이 포함됩니다.

- OpenSSL(지원되는 버전: 8.3)

  PHP의 OpenSSL 확장은 다양한 암호화 작업을 위해 OpenSSL 라이브러리의 기능을 구현합니다. 이 라이브러리에 대한 확장 지원에는 암호화 키 쌍에 대한 개선된 데이터 흐름 지원이 포함됩니다.

- Simdjson(지원되는 버전: 8.3)

  PHP의 Simdjson 확장은 simdjson 프로젝트의 PHP 특정 바인딩을 구현하여 빠른 JSON 디코딩을 제공합니다. 최초 지원에는 다음과 같은 신규 PHP 범주가 포함됩니다.

  - JSON Path Manipulation

iOS에 대한 지원 개선(지원되는 버전: 17)[2]

개발자는 Apple iOS 및 iPadOS SDK에서 제공되는 프레임워크 컬렉션을 사용하여 Apple iPhone과 iPad 장치용 모바일 응용 프로그램을 빌드할 수 있습니다. 이번 릴리스에서는 Swift 및 Objective-C용 iOS SDK 지원이 증분 방식으로 업데이트되었습니다. 신규 규칙과 업데이트된 규칙을 적용하면 iOS 17에서 다음 프레임워크의 API 적용 범위를 확장할 수 있습니다.

- CryptoKit

[2] iOS 17 API에는 Xcode 15 이상이 필요하며, 이는 Fortify Static Code Analyser 23.2 이상이 필요합니다. 그러나 Source Code Analyzer 23.2를 사용하여 iOS 17 API를 사용하는 앱을 빌드하는 경우 컴파일러 경고가 발생할 수 있습니다. 유효한 컴파일 및 스캔을 보장하려면 Fortify Static Code Analyzer 24.2 이상을 사용하는 것이 좋습니다.

- Foundation
- Network
- os
- System
- SwiftUI
- UIKit

이러한 업데이트를 설치하면 다음과 같은 취약성 범주에서 문제를 더욱 정확하게 감지할 수 있습니다.

- Insecure Transport
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- System Information Leak: External
- System Information Leak: Internal
- Unreleased Resource: Synchronization
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: User-Controlled Salt
- Weak Encryption: User-Controlled Key Size

MISRA C 2012에 대한 지원 개선

MISRA는 소프트웨어의 높은 무결성 또는 높은 안정성이 필요한 안전이 중요한 환경에서 사용되는 응용 프로그램 개발을 위한 다양한 표준을 만들고 유지 관리하는 표준 조직입니다. 이번 릴리스에는 MISRA C 2012 표준의 두 가지 필수 지침 규칙에 강력하게 매핑되는 두 가지 신규 범주에 대한 지원이 포함되어 있습니다.

- Undefined Behavior: File Pointer Dereference
- Undefined Behavior: File Pointer Use After Close

비밀번호 정규식 속성 업데이트

Fortify Static Code Analyser 버전 23.1에 도입된 비밀번호 정규식 속성은 Fortify 규칙이 여러 언어의 비밀번호 식별자와 일치하는 방식을 지정하는 정규식이 포함된 사용자 지정 가능한 속성입니다. 이번 릴리스에서는 "secret"이라는 단어가 포함된 비밀번호 식별자를 인식하도록 com.fortify.sca.rules.password_regex.global 속성의 기본값을 확장했습니다. 또한 동적으로 생성된 JSON 문자열 분석 시 비밀번호 정규식 속성을 활용하는 새로운 규칙을 추가했습니다. 결과적으로 언어 전반에 걸쳐 다음 범주에서 감지 기능이 개선됩니다.

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Privacy Violation

Golang에 대한 지원 개선(지원되는 버전: 최대 1.21)

Golang이라고도 하는 Go는 Google에서 만든 컴파일된 정적인 유형의 프로그래밍 언어입니다. 단순성, 효율성 및 동시성에 대해 강력하게 지원하는 것으로 잘 알려져 있어 확장 가능한 웹 서비스, 데이터 파이프라인 및 분산 시스템을 구축하는 데 적합합니다. 이번 릴리스에서는 *Unreleased Resource* 취약성에 대한 감지 기능이 포함되며, GORM v2를 사용하는 프로젝트에 대한 새로운 *SQL Injection* 감지 기능이 도입됩니다.

WordPress API 개선 사항(지원되는 버전: 최대 6.5)(API 개수: 2)

WordPress API(Application Programming Interface)는 여러 API 섹션/주제로 분리될 수 있으며, 각각은 주어진 기능 세트와 관련된 기능과 사용을 다루고 있습니다. 이는 함께 전체 WordPress 프로젝트에 의해 생성된 플러그인/테마/추가 인터페이스인 WordPress API라고 불리는 것을 형성합니다. 이번 릴리스에서는 다음 API에서 문제를 식별하기 위한 최초 지원이 추가되었습니다.

- REST API
- Shortcode API

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.

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 MVC Bad Practices: Optional Submodel With Required Property* – ASP.NET 응용 프로그램에서 오탐지 감소
- *Insecure Transport: Mail Transmission* – Java 응용 프로그램에서 오탐지 감소
- *Password Management: Hardcoded Password* – JSON/YAML 파일에서 오탐지 감소
- *Unreleased Resource: Streams* – Java 응용 프로그램에서 오탐지 감소
- *Password Management: Hardcoded Password* – Dictionary 유형과 관련된 Python 응용 프로그램에서 신규 문제 감지
- *Password Management: Hardcoded Password* – 보간된 문자열과 관련된 ASP.NET 응용 프로그램에서 신규 문제 감지
- 내장된 JDK 시스템 속성에서 발생하는 여러 가지 오탐지 현상 해소

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 3개 범주의 이름이 변경되었습니다.

2024 R1 범주 이름	2024 R2 범주 이름
Access Control: gRPC Authentication Bypass	Access Control: gRPC Fail Open
AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS CloudFormation Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key
AWS Terraform Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key

DISA CCI(Control Correlation Identifier) 버전 2

DISA(Defense Information Systems Agency) CCI는 실행 가능한 단일 문과 함께 표준 식별자 세트를 페어링하여 높은 수준과 낮은 수준의 사이버 보안 지침 간의 격차를 해소하는 문서입니다. DISA 응용 프로그램 보안 및 개발 STIG는 단일 STIG 제어가 하나 이상의 CCI에 적용될 수 있는 DISA CCI에 밀접하게 매핑됩니다. 이번 릴리스에서는 매핑된 CCI를 이전 릴리스에서 Fortify Taxonomy에 대한 STIG 매핑의 최신 업데이트와 동일하게 만듭니다.

NIST Special Publication 800-53 개정 4 및 5

NIST(National Institute of Standards and Technology) Special Publication 800-53은 시스템을 보호하는 방법에 대한 지침을 제공하기 위해 사이버 보안 분야에서 전반적으로 활용할 수 있는 정보 시스템에 대한 보안 및 개인 정보 보호 제어 범주를 제공하는 문서입니다. NIST Special Publication 800-53은 DISA CCI와 밀접하게 매핑되어 있으며, 단일 CCI가 하나 이상의 NIST 800-53 제어에 적용될 수 있습니다. 이번 릴리스에서는 매핑된 NIST 800-53 제어를 Fortify Taxonomy에 대한 DISA CCI 매핑의 최신 업데이트와 동일하게 만듭니다.

OWASP Mobile Top 10 2023

이전에 발표된 대로 Fortify 소프트웨어 보안 콘텐츠의 이번 릴리스에서는 이제 OWASP Mobile Top 10 2023 매핑 사용이 중단되며, 업데이트된 OWASP Mobile Top 10 2024만 남게 됩니다.

OpenText 버전 관리에 맞춰 소프트웨어 보안 콘텐츠 릴리스 조정

다음 릴리스에는 보안 콘텐츠 버전 관리에 대한 변경 사항이 포함될 예정입니다. 이는 "2024 업데이트 2"의 명명 규칙을 따르는 마지막 OpenText Fortify 보안 콘텐츠 업데이트 릴리스입니다. OpenText 버전 관리 표준에 맞추기 위해 릴리스는 매년 분기별로 하나씩 예정되어 있으며, 연도 및 분기에 따라 번호가 지정됩니다. 따라서 OpenText™ Fortify™ 소프트웨어 보안 콘텐츠 릴리스의 다음 릴리스는 24.4이며, 이는 2024년 4분기 첫 번째 달의 릴리스임을 나타냅니다.

Fortify SecureBase [Fortify WebInspect]

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

취약점 지원

Denial of Service: GraphQL

API용 GraphQL 쿼리 언어는 기존 데이터를 쿼리하는 런타임을 제공합니다. GraphQL 스키마는 데이터 개체, 해당하는 필드 및 유형, 다른 데이터 개체와의 관계로 구성된 모델입니다. 다른 데이터 개체 간의 참조는 순환을 만들 수 있습니다. 공격자는 DoS(Denial of Service)를 유발하는 악의적인 중첩 및 비용이 많이 드는 순환 쿼리를 작성하여 과도한 CPU 및 메모리 사용을 트리거할 수 있습니다. 이번 릴리스에는 GraphQL 스키마의 순환 참조를 감지하는 검사 기능이 포함되어 있습니다.

Access Control: Authorization Bypass(CVE-2024-27198)

CVE-2024-27198은 JetBrains 소프트웨어의 치명적인 취약점으로 식별되었으며, 심각한 보안 위협을 나타냅니다. 이 취약점은 인증되지 않은 공격자가 영향을 받는 시스템에 대한 관리 제어를 얻을 수 있도록 허용하는 불충분한 인증 메커니즘과 관련된 위험을 강조합니다. 최신 릴리스에는 대상 서버에서 이 취약점을 감지하는 검사 기능이 포함되어 있습니다.

Directory Traversal(CVE-2024-27199)

2023.11.4 이전의 JetBrains TeamCity On-Premises 서버 버전은 CVE-2024-27199로 식별되는 Path Traversal 결함에 취약합니다. 공격자는 이 결함을 이용해 인증 제어를 우회하고, 시스템 무결성과 기밀성을 크게 위협할 수 있습니다. 최신 릴리스에는 대상 서버에서 이 취약점을 감지하는 검사 기능이 포함되어 있습니다.

Dynamic Code Evaluation: 안전하지 않은 역직렬화(CVE-2023-26360)

Adobe ColdFusion 버전 2018 업데이트 15 이하 및 2021 업데이트 5 이하는 CVE -2023-26360으로 식별된 Dynamic Code Evaluation 취약점의 영향을 받습니다. 이 취약점으로 인해 현재 사용자의 컨텍스트에서 임의 코드가 실행될 수 있습니다. 이 문제를 악용하는 데에는 사용자 상호 작용이 필요하지 않습니다. 이번 릴리스에는 대상 서버에서 이 취약성을 감지하는 검사 기능이 포함되어 있습니다.

Insecure Deployment: Unpatched Application(CVE-2024-32962)

CVE-2024-32962는 Node.js용 XML 디지털 서명 및 암호화 라이브러리인 xml-crypto와 관련된 치명적인 취약점입니다. 이 취약점은 버전 4.0.0에서 발생했으며, 버전 6.0.0에서 해결되었습니다. 취약점은 영향을 받는 버전에서 기본 구성이 서명자의 인증을 확인하지 않기 때문에 발생합니다. 공격자는 XML 문서를 수정하고, 기존 서명을 악성 개인 키로 생성된 서명으로 대체하고, 해당 인증서를 <KeyInfo/> 요소에 첨부하여 이를 악용할 수 있습니다. 이번 릴리스에는 영향을 받는 xml -crypto 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 다음 영역에서 보고된 검사 결과를 해결하기 위해 변경된 사항도 확인할 수 있습니다.

Insecure Deployment: OpenSSL

이번 릴리스에는 오탐지를 줄이고 결과의 정확성을 높일 수 있도록 개선된 OpenSSL ChangeCipherSpec MitM(Man-in-the-Middle) 기능이 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.

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