Micro Focus

Fortify 소프트웨어 보안 콘텐츠

2020 업데이트 2

2020 년 6 월 26 일 금요일

Micro Focus Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구 결과를 보안 인텔리전스로 변환하여 Fortify Static Code Analyzer(SCA), Fortify WebInspect 및 Fortify Application Defender 를 포함한 Fortify 제품 포트폴리오를 강화합니다. 현재 Micro Focus Fortify 소프트웨어 보안 콘텐츠는 27 개의 프로그래밍 언어에서 1,022 개의 취약점 범주를 지원하며 1 백만 개 이상의 개별 API 를 지원합니다.

자세한 내용: https://software.microfocus.com/en-us/software/security-research

Fortify SSR(Software Security Research)은 Fortify Secure Coding Rulepacks(영어, 버전 2020.2.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능) 및 Fortify Premium Content 의 업데이트를 바로 사용할 수 있다는 점을 알려 드립니다.

Micro Focus Fortify Secure Coding Rulepacks[SCA]

이 릴리스에서 Fortify Secure Coding Rulepacks 는 27 개의 프로그래밍 언어에서 810 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Kotlin 코어 라이브러리 지원(버전 1.3)[1]

JVM 을 대상으로 하는 다음 패키지를 포함하는 Kotlin 표준 라이브러리에 대한 초기 지원:

- Kotlin
- kotlin.collections
- kotlin.comparisons
- kotlin.io
- kotlin.properties
- kotlin.random
- kotlin.ranges
- kotlin.sequences
- kotlin.streams
- kotlin.text

제한된 Java 상호 운용성은 Java 에서 지원하는 모든 범주 및 라이브러리가 Kotlin 에서는 모두 부분적으로 지원되며 다음은 Kotlin 표준 라이브러리에 대해 특별히 지원된다는 것을 의미합니다.

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial of Service: Regular Expression
- Denial of Service: StringBuilder
- Formula Injection
- Insecure SSL: 지나치게 폭넓은 인증서 트러스트
- 로그 위조
- Path Manipulation
- 취약한 로깅 관행: 시스템 출력 스트림 사용
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak
- 시스템 정보 누출: External
- 시스템 정보 누출: Internal
- 트러스트 경계 위반
- 확인되지 않은 반환 값

[1] SCA 20.1.2 패치 릴리스가 필요합니다. SCA 20.1 을 사용하면 규칙 및 특정 Lambda 함수와 관련된 여러 가지 오류가 발생하며 패치 릴리스에서는 이러한 오류가 발생하지 않습니다.

C# 8 및 .NET Core 개선 사항

버전 2.1, 2.2, 3.0 및 3.1 을 포함하여 C# 8 및 .NET Core 라이브러리에 대한 지원이 업데이트되었습니다. 이를 통해 .NET Standard 2.1 에 대한 완전한 규칙 지원과 C# 8 의 비동기 *foreach*, *range* 및 *using* 작업 사용 시 개선된 데이터 흐름이 제공됩니다.

Python 코어 라이브러리 개선 사항[2]

버전 3.7 및 3.8 을 포함한 Python 코어 라이브러리에 대한 지원이 업데이트되었습니다. 이전에 지원되던 범주에 더해 이제 다음과 같은 새로운 범주가 지원됩니다.

- Python Bad Practices: Leftover Debug Code

Go 코어 라이브러리 지원 개선 사항(버전 1.13)

crypto/tls 를 포함하도록 Go 코어 라이브러리에 대한 지원이 확장되었습니다. Google™에서 설계한 정적 유형의 오픈 소스 언어인 Go 를 사용하면 간단하고 안정적이며 효율적인 소프트웨어를 쉽게 구축할 수 있습니다. Go 는 C 와 구문이 비슷하지만 메모리 안전 메커니즘, 가비지 수집 및 구조적 입력 기능을 제공합니다. 지원되는 범주에는 다음이 포함됩니다.

- Insecure SSL: Server Identity Verification Disabled
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- 시스템 정보 누출: External

GORM(버전 1.9.12)

Jinzhu 가 작성한 Golang 용 오픈 소스 ORM(Object Relational Mapping) 프로젝트인 GORM 라이브러리 지원. GORM 은 엔터프라이즈 애플리케이션에 데이터베이스 관련 위험을 유발할 수 있는 공통 ORM 라이브러리입니다. 지원되는 범주에는 다음이 포함됩니다.

- Access Control: Database
- Connection String Parameter Pollution
- Dynamic Code Evaluation: Code Injection
- Insecure Transport
- 로그 위조
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Privacy Violation
- Setting Manipulation
- SQL Injection
- 시스템 정보 누출: Internal
- 취약한 암호화 해시

[2] 프로젝트에 할당 식과 같은 새로 도입된 구문이 포함된 경우 개선된 결과를 얻기 위해 SCA 20.2 가 필요합니다.

OWASP ASVS 4.0

appsec 프로그램을 실행하는 데 도움이 되는 프레임워크를 찾는 고객을 지원하기 위해 이 릴리스에서는 Micro Focus Fortify Taxonomy 범주와 OWASP 애플리케이션 보안 검증 표준 버전 4.0 요구 사항 간의 상관 관계를 지원합니다. ASVS 는 고객이 보안 애플리케이션의 정의, 구축, 테스트 및 검증을 지원하는 데 사용할 수 있는 요구 사항 또는 테스트 목록을 제공합니다.

기타 정정표

이번 릴리스에서는 거짓 긍정 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.

영역 변경 사항:

일부 지역에서는 일관성을 위해 특정 범주의 영역이 변경되었습니다. 이로 인해 이전 버전의 SCA(6.30 이전 버전, 즉 2015-04-17 이전의 모든 릴리스)에서는 병합 시 일부 문제가 "업데이트 됨"으로 유지되는 대신 새로운 문제/제거된 문제로 처리될 수 있습니다. SCA 6.30 이상의 모든 버전에서는 이 문제가 발생하지 않습니다.

사용자가 영역별로 필터링하는 경우 일반적으로 필터링에도 영향을 미칠 수 있습니다. 영향을 받는 범주에는 다음이 포함됩니다.

- Access Control: ACL 조작. "입력 유효성 검사 및 표현"에서 "보안 기능"으로 변경됨
- Access Control: Authorization Bypass. "입력 유효성 검사 및 표현"에서 "보안 기능"으로 변경됨
- 시스템 정보 누출: Struts 2 "입력 유효성 검사 및 표현"에서 "캡슐화"로 변경됨

거짓 긍정 개선 사항:

당사는 고객의 소리에 귀를 기울이고 거짓 긍정의 비율을 개선하기 위해 노력하고 있습니다. 이 릴리스에서는 거짓 긍정의 수를 줄이기 위해 다음과 같은 작업을 수행했습니다.

- 여러 범주에서 거짓 긍정을 일으키는 특정 JavaScript 소스 규칙을 제거했습니다.
- Java "릴리스되지 않은 리소스: 데이터베이스" 규칙이 JDBC 4.3 사양에 따라 기본 리소스를 닫는 연결을 고려하도록 개선되었습니다.
- Java File.createTempFile()에서 거짓 긍정 "경로 조작" 문제를 제거했습니다.
- TypeScript 정의 파일에서 문제 보고가 비활성화되었습니다.
- SendAsync 에서 일부 .NET "Server-Side Request Forgery"가 제거되었습니다.
- Java "Spring 보안 구성 오류: Incorrect Request Matcher Type" 거짓 긍정의 수가 줄어들었습니다.
- 중복된 .NET "취약한 암호화" 문제가 제거되었습니다.
- 문자열 유형에 대한 .NET "ASP.NET Bad Practices: Non-Serializable Object Stored in Session" 거짓 긍정이 제거되었습니다.
- 의도하지 않은 net.http.Response 개체 오염으로 인한 Golang 거짓 긍정이 제거되었습니다.
- Java 내에서 드물게 발생하는 "코드 정확성: Class Does Not Implement equals" 거짓 긍정이 확인되고 제거되었습니다.
- JavaScript 에서 여러 가지 거짓 긍정 "키 관리" 문제가 제거되었으며 이후 릴리스에서 추가 처리가 계속될 것입니다.

오류 및 경고:
전체 2020.2.0 규칙 팩과 함께 사용할 경우 SCA 19.2 에서 지원되는 모든 프로그래밍 언어에 대해 검사 중 규칙 로드로 인해 빌드 및 검사 로그에 다음 경고가 생성됩니다.

```
[WARN  20599]
The rule language kotlin has no corresponding mapping in SCA
```

이는 SCA 19.2 의 알려진 문제이며 다음 Kotlin 규칙 팩 파일을 제거하여 해결할 수 있습니다.
<FORTIFY_DIR>\Fortify_SCA_and_Apps_19.2.0\Core\config\rules\core_kotlin.bin
Kotlin 을 검사하려면 SCA 20.1.2 가 필요합니다.

VulnCat 개선 사항
항목이 논리적 순서로 표시되도록 필터 범주 및 필터 하위 범주의 정렬이 개선되었습니다.

ESAPI 유효성 검사 지원
당사는 고객의 의견에 늘 귀를 기울이고 있으며 많은 사람들이 라이브러리에 대한 보안 문제로 인해 ESAPI API 가 문제를 해결하도록 허용하는 SCA 규칙에 대해 우려하고 있습니다.
이번 릴리스부터 ESAPI 라이브러리에서 유효성 검사를 제거했으며 이제 데이터 흐름 문제가 나타나지 않도록 인코딩 기능을 통해 데이터 흐름이 계속됩니다.
일부 고객의 경우 특히 레거시 제품에서 ESAPI 라이브러리를 계속 사용하고 싶어한다는 점을 잘 알고 있으며, 그에 따라 이 유효성 검사를 다시 포함할 수 있는 별도의 규칙 팩을 만들고 있습니다.

ESAPI 를 계속 사용하려는 경우 지원 포털의 Premium Content, Fortify Exchange 에서 ESAPI 확장 규칙 팩을 사용할 수 있습니다.

또한 이 업데이트에서는 "Obsolete: Deprecated by ESAPI"로 표시되는 모든 문제가 제거되었으며, 이는 위에서 언급한 별도의 규칙 팩을 사용해서도 찾을 수 있습니다.

취약한 암호화 업데이트
공식적으로 TDEA(Triple Data Encryption Algorithm)라고도 하는 3DES 는 이제 NIST(National Institute of Standards and Technology)의 권장 사항에 따라 취약한 암호화로 보고됩니다.

Micro Focus 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

웹 서버 구성 오류: 정보 공개

Spring Boot 에는 관리자가 웹 애플리케이션을 모니터링하고 관리할 수 있는 액추에이터라고 하는 여러 추가 기능이 포함되어 있습니다. 이번 릴리스에는 권한이 없는 사용자가 사용할 수 있는 민감한 Spring Boot Actuator 를 감지하는 검사가 포함되어 있습니다. 이러한 액추에이터 엔드포인트를 사용하여 공격자는 감사, 상태 및 메트릭 정보를 수집하거나 일부 구성에서 원격 코드 실행 공격을 감행할 수도 있습니다.

Cross-Site Scripting: Reflected

ASP.NET API ResolveUrl 은 런타임에 app-root-relative 경로를 확인하는 데 사용됩니다. API 는 쿠키가 없는 상태 ID 형식 값을 포함하는 상대 경로의 유효성을 검사하지 못하며, 그에 따라 공격자가 애플리케이션에 대해 교차 사이트 스크립팅 공격을 감행할 수 있습니다. 이 릴리스에는 .NET 애플리케이션에서 이러한 취약성을 감지하는 검사 기능이 포함되어 있습니다.

Cookie Security: SameSite 특성 누락

쿠키의 SameSite 특성은 Cross-Site Request Forgery 공격으로부터 애플리케이션을 보호하는 간단한 메커니즘을 제공합니다. 최신 브라우저 버전에서는 SameSite 특성이 설정되지 않은 쿠키가 거부될 수 있습니다. 이 릴리스에는 SameSite 특성 설정에 실패한 쿠키 설정 인스턴스를 감지하는 검사가 포함되어 있습니다.

Cookie Security: 잘못 구성된 접두사

이름이 _Host- 또는 _Secure-로 시작하는 쿠키는 호스트 수준 제한을 적용하며, 우발적인 도청 및 스푸핑으로부터 보호하기 위해 보안 HTTPS 연결을 통해서만 전송되어야 합니다. Path, Domain 및 Secure 특성이 적절하게 설정되지 않은 쿠키는 브라우저에서 거부될 수 있습니다. 이 릴리스에는 잘못 구성된 접두사가 있는 쿠키를 감지하는 검사가 포함되어 있습니다.

Cookie Security: Overly Permissive SameSite 특성

쿠키의 SameSite 특성 값이 Strict 일 경우, 브라우저에서 도메인에 대한 최상위 탐색의 결과로 발생한 요청에만 해당 쿠키가 추가됩니다. 또는 동일한 호스트가 iframe, link, form 등의 링크가 있는 다양한 HTML 태그에서 요청할 때에만 요청에 해당 쿠키를 추가합니다. 애플리케이션을 Cross-Site Request Forgery 공격으로부터 최대한 보호하려면 세션 ID 의 SameSite 특성에 대해 Strict 값을 설정해야 합니다. 이 릴리스에는 세션 쿠키에 대해 SameSite 특성이 Strict 로 설정되지 않은 인스턴스를 감지하기 위한 검사가 포함되어 있습니다.

컴플라이언스 보고서

OWASP ASVS(Application Security Verification Standard)

OWASP ASVS 는 보안 제어를 위해 웹 애플리케이션을 테스트하는 방법 및 안전한 개발 지침을 제공합니다. 이 릴리스에는 OWASP ASVS 4.0 의 최신 버전과 WebInspect 검사의 상관 관계가 포함되어 있습니다.

정책 업데이트

OWASP ASVS(Application Security Verification Standard) 정책

WebInspect 검사와 OWASP ASVS 최신 버전의 상관 관계 외에도 이 릴리스에는 OWASP ASVS 와의 상관 관계를 유발하는 취약성을 식별하는 정책도 포함되어 있습니다.

기타 정정표:

이번 릴리스에서는 거짓 긍정 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.

- Often Misused 에 대한 보안 콘텐츠 개선: 취약한 SSL 인증서에 인증서가 취약한 것으로 간주되는 이유에 대한 정보가 보다 정확하게 반영됩니다. ID 가 11635 인 새로운 검사가 추가되었습니다.

Micro Focus Fortify Premium Content

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

OWASP ASVS(Application Security Verification Standard):

ASVS(Application Security Verification Standard)는 안전한 소프트웨어를 구축하기 위한 SDLC(소프트웨어 개발 수명 주기) 및 구성 과정에서 수행할 테스트 및 애플리케이션 보안 요구 사항이 포함되어 있는 목록입니다. 당사는 업계 파트너와 협력하여 매핑 설계 방식을 개선함에 따라 매핑이 계속 발전할 것으로 예상합니다. 새로운 상관 관계를 지원하기 위해, 이 릴리스에는 PCI SSF 4.0 을 지원하는 Fortify SSC 에 대한 새로운 보고서 번들이 포함되어 있습니다. 보고서 번들은 Fortify 고객 포털의 Premium Content 에서 다운로드할 수 있습니다.

Micro Focus 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 Micro Focus Fortify 지원 포털에서 얻을 수 있습니다.

Fortify 기술 지원 연락처
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR 연락처
Alexander M. Hoole
Software Security Research, 관리자
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

© Copyright 2020 Micro Focus or one of its affiliates. The information contained herein is subject to change without notice. The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

2020 년 6 월 26 일