Fortify 소프트웨어 보안 콘텐츠

2021 업데이트 3

2021 년 9 월 24 일

CyberRes Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구 결과를 보안 인텔리전스로 변환하여 Fortify Static Code Analyzer, Fortify WebInspect 및 Fortify Application Defender 를 포함한 Fortify 제품 포트폴리오를 강화합니다. 현재 CyberRes Fortify 소프트웨어 보안 콘텐츠는 27 개의 프로그래밍 언어에서 1,051 개의 취약점 범주를 지원하며 1 백만 개 이상의 개별 API 를 지원합니다.

Fortify SSR(Software Security Research)은 Fortify Secure Coding Rulepacks(영어, 버전 2021.3.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능) 및 Fortify Premium Content 의 업데이트를 바로 사용할 수 있다는 점을 알려 드립니다.

CyberRes Fortify Secure Coding Rulepacks [Static Code Analyzer]

이 릴리스에서 Fortify Secure Coding Rulepacks 는 27 개의 프로그래밍 언어에서 831 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Golang 표준 라이브러리 업데이트(버전: 1.16)

Go 표준 라이브러리 지원 범위가 확대되었습니다. 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. 이 업데이트는 표준 라이브러리 네임스페이스에 적용되며 새로운 범주에 대한 지원을 추가합니다.

- Cookie Security: SameSite 특성 누락
- Cookie Security: Overly Permissive SameSite 특성
- Go Bad Practices: Leftover Debug Code
- Insecure Randomness: 하드코딩된 시드
- Insecure Randomness: User-Controlled Seed
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Protocol
- Often Misused: Privilege Management
- 취약한 암호화 서명

Android 11 업데이트(API 레벨: 30)

Android 플랫폼은 모바일 장치용으로 설계된 오픈 소스 소프트웨어 스택입니다. Android 의 주요 구성 요소는 응용 프로그램 개발자에게 Android 기능을 제공하는 Java API Framework 입니다. 이 릴리스는 Android 의 Java API Framework 를 활용하는 Java 또는 Kotlin 으로 작성된 기본 Android 응용 프로그램에서 취약성 탐지를 확장합니다. 사용자는 Android 응용 프로그램 모델링 및 API 적용 범위에 대한 업데이트에서 향상된 결과를 기대할 수 있습니다. 또한 이 릴리스에는 위험한 Android 사용 권한에 대한 지침을 제공하는 다음과 같은 새로운 권한 관리 취약성 범주가 포함되어 있습니다.

- Privilege Management: Android Activity Recognition
- Privilege Management: Android Calendar
- Privilege Management: Android Call Log

- Privilege Management: Android Camera
- Privilege Management: Android Contacts
- Privilege Management: Android Microphone
- Privilege Management: Android Sensors

iOS 표준 라이브러리 업데이트(버전: iOS 14)

이 릴리스는 Swift 와 Objective-C 모두에 대해 iOS 14 라이브러리 API 지원을 업데이트합니다. 업데이트는 다음 프레임워크에 초점을 맞추고 있습니다.

- UIKit
- UserNotification
- SwiftUI
- MessageUI

사용자는 Insecure IPC, Link Injection, Path Manipulation, Privacy Violation, Shoulder Surfing 및 System Information Leak 범주에서 개선을 기대할 수 있습니다.

Micro Focus Visual COBOL 업데이트(버전: 7.0)

다음 두 가지 취약성 범주에 대한 지원을 추가하기 위해 Micro Focus Visual COBOL 버전 7 에 대한 지원이 확장되었습니다.

- Integer Overflow
- Race Condition: File System Access

SAPUI5/OpenUI5 지원 [1](버전: 1.93)

SAPUI5 는 SAP 에 의해 만들어진 클라이언트 측 JavaScript 프레임워크로, 핵심 제어 라이브러리 집합을 오픈 소스 OpenUI5 와 공유합니다. 이 릴리스는 다음 범주에 대한 취약성을 식별하는 초기 지원을 제공합니다.

- Cross-Site Scripting: DOM
- Cross-Site Scripting: SAPUI5 Control
- Cross-Site Scripting: Self
- Privacy Violation
- SAPUI5 Misconfiguration: Unsanitized Editor
- 시스템 정보 누출: External

[1] Static Code Analyzer v21.2.0 이상을 사용할 때 향상된 결과를 기대할 수 있습니다.

JSON 지원 [2]

JSON(JavaScript Object Notation)은 간단한 데이터 교환 형식입니다. 이 릴리스는 다음 범주에 대해 JSON 의 취약성을 식별하는 향상된 지원을 제공합니다.

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Password in Comment[3]

Kotlin 표준 라이브러리 업데이트(버전: 1.4.30)

Kotlin 은 Java 상호 운용성을 갖춘 정적 유형의 범용 언어입니다. 이 릴리스에는 JVM(Java Virtual Machine)을 대상으로 Kotlin 1.4 에 도입된 새로운 표준 라이브러리 API 에 대한 업데이트된 지원이 포함되어 있습니다.

ECMAScript 2021(버전: ECMA-262)

ECMAScript 2021 에서는 새로운 API 에 대한 지원이 도입되었습니다. ECMAScript 는 ECMAScript 언어 사양이 정의하는 범용 프로그래밍 언어로, 모든 최신 웹 브라우저에 통합되는 것으로 가장 잘 알려져 있습니다. 하지만 웹 서버, 모바일 응용 프로그램 및 기타 유형의 기존 응용 프로그램을 빌드하기 위해 사용되는 경우가 점점 더 흔해지고 있습니다. 고객은 최신 ECMAScript 표준을 대상으로 하는 응용 프로그램을 검색할 때 향상된 데이터 흐름을 기대할 수 있습니다.

2021 CWE™(Common Weakness Enumeration) Top 25

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Weaknesses(CWE Top 25)는 2019 년에 도입되었으며 SANS Top 25 를 대체합니다. 7 월에 릴리스된 2021 CWE Top 25 는 지난 2 년 동안 NVD(National Vulnerability Database)에 보고된 취약점의 빈도 및 심각도를 정규화하는 추론적 공식을 사용하여 결정되었습니다. NVD 에서 가장 일반적으로 보고된 치명적인 취약점을 중심으로 감사의 우선 순위를 지정하고자 하는 고객을 지원하기 위해, CyberRes Fortify Taxonomy 와 2021 CWE Top 25 사이의 상관 관계가 추가되었습니다.

---

[2] Static Code Analyzer v21.1.0 및 플래그: '-Dcom.fortify.sca.use.json-analyzer=true'가 필요합니다.

[3] Static Code Analyzer v21.2.0 이상이 필요합니다. Static Code Analyzer v21.2.0 부터는 플래그가 필요하지 않습니다.

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.

18.x 이전 Static Code Analyzer 버전의 사용 중단:

2020.4 릴리스에서 관찰된 바와 같이, 마지막 4 가지 Static Code Analyzer 주 릴리스가 계속 지원됩니다. 따라서 이것은 18.x 이전 Static Code Analyzer 버전을 지원하는 Rulepacks 의 마지막 릴리스입니다. 다음 릴리스에서는 18.x 이전 Static Code Analyzer 버전에서 최신 Rulepacks 가 로드되지 않습니다. 따라서 Rulepacks 를 다운로드하거나 Static Code Analyzer 버전을 업그레이드해야 합니다.
향후 릴리스에서는 Static Code Analyzer 의 마지막 4 가지 주 릴리스가 계속해서 지원됩니다.

Java J2EE 개선 사항:

Privacy Violation 및 *System Information Leak* 범주에서 javax.servlet API 에 대한 지원이 개선되었습니다.

Android Bound Services:

Android 가 계속 지원됨에 따라 이 릴리스에는 Android Bound Services 의 적용 범위가 포함되어 있습니다. 고객은 Android Bound Service 메서드 매개 변수에서 비롯되는 새로운 데이터 흐름 문제를 예상할 수 있습니다. 이로 인해 바인딩된 서비스 내에서 메서드가 호출될 때 중복된 데이터 흐름 하위 트레이스가 발생할 수 있습니다.

Node.js 에 있는 약한 암호화 해시:

Node.js 응용 프로그램에서 약한 암호화 해시 사용을 식별합니다.

이제 OWASP ASVS 4.0 매핑에 레벨 지원이 포함됨

특정 OWASP ASVS(Application Security Verification Standard) 응용 프로그램 보안 확인 레벨(L1, L2 및 L3)을 위반하는 보고된 문제를 쿼리할 수 있기를 원하는 고객을 지원하기 위해 최신 보안 콘텐츠는 이러한 레벨을 매핑 이름에 추가했습니다. 고객은 이제 *OWASP ASVS 4.0* 그룹화 내에서 관련 *L1*, *L2* 및 *L3* 키워드를 검색하는 것은 물론 AuditWorkbench 및 SSC(Software Security Center)에서 사용할 관련 filterset 및 filtertemplate 을 설계할 수 있습니다.

오탐지 개선 사항:

이 릴리스에서는 오탐지를 제거하기 위한 작업이 계속되었습니다. 다른 개선 사항을 기반으로 다음 영역의 오탐지가 추가로 제거됩니다.

- jQuery 코드의 *Cross-Site Scripting* 오탐지
- *Privacy Violation: Shoulder Surfing*(.NET 응용 프로그램에 있으며 JsonIgnore 특성을 사용함)
- 숫자만 제어할 수 있는 *Path Manipulation* 문제에서 Fortify Priority Order 를 낮추기 위한 일관성 향상
- 암호가 열거의 일부인 경우 Swift 에서 더 이상 암호를 식별하지 않음
- .NET 의 *Missing XML Validation* 문제
- Java 프로젝트의 *Missing Check against Null*

CyberRes 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

Insecure Deployment: HTTP Request Smuggling

HTTP2 over clear text smuggling 또는 h2c smuggling 은 프록시 서버와 같이 h2c 를 인식하지 못하는 프런트 엔드를 오용하여 백엔드 시스템으로의 터널을 만드는 전형적인 HTTP request smuggling 의 대안입니다. 공격자는 이 터널을 사용하여 프런트 엔드 서버에 들키지 않고 백엔드 서버로 추가 요청을 몰래 반입할 수 있습니다. 이를 통해 공격자는 프런트 엔드의 권한 부여 제어를 우회하고 백엔드 시스템의 제한된 리소스에 액세스할 수 있습니다. 이 릴리스에는 h2c smuggling 공격에 사용될 수 있는 구성을 탐지하는 검사가 포함되어 있습니다.

Access Control: Missing Authorization Check

GraphQL Introspection 을 사용하면 서버를 쿼리하여 기본 스키마에 대한 정보를 얻을 수 있습니다. Introspection 은 쿼리, 유형, 필드 등의 요소에 대한 세부 정보를 제공합니다. 흔히 GraphQL Introspection 은 기본적으로 활성화되어 있습니다. 적절한 권한이 없는 공격자는 SQL 삽입 및 일괄 처리 공격과 같은 공격을 위해 이 정보를 오용할 수 있습니다. 이 릴리스에는 introspection 기능이 활성화된 GraphQL 엔드포인트를 탐지하는 검사가 포함되어 있습니다.

NoSQL Injection: MongoDB

NoSQL 스크립트 삽입 취약성을 통해 공격자는 데이터베이스에 악성 쿼리를 삽입할 수 있습니다. MongoDB 는 NoSQL 데이터베이스 중 하나이며, 응용 프로그램이 JavaScript 작업을 실행할 수 있도록 허용하는 것으로 알려져 있습니다. 권한을 부여받지 않은 공격자가 데이터를 추출하거나 JavaScript 코드를 실행할 수 있으므로 NoSQL 삽입은 매우 위험합니다. 이로 인해 원격 코드 실행, 기밀성 손상, 응용 프로그램 데이터 무결성, 서비스 거부(DoS) 공격이 발생할 수 있습니다. 이 릴리스에는 MongoDB 에서 NoSQL 스크립트 삽입을 탐지하는 검사가 포함되어 있습니다.

Dynamic Code Evaluation: 안전하지 않은 역직렬화

7.0 이전 ForgeRock AM 그리고 14.6.4 이전 OpenAM 에서 사전 권한 부여 안전하지 않은 Java 역직렬화 취약성이 CVE-2021-35464 에 의해 발견되었습니다. 이 취약성은 공격자가 jato.pageSession 매개 변수에서 악성 직렬화 개체를 만들어서 단일 요청을 통해 엔드포인트 "/ccversion/Version"에 전송하는 것을 허용합니다. 이 취약성은 응용 프로그램에서 안전하지 않은 타사 Java 라이브러리를 사용함으로써 발생합니다. 일반적으로 공격자는 이 문제를 이용하여 서버에서 임의 코드를 실행하거나, 응용 프로그램 논리를 오용하거나, 서비스 거부(DoS) 공격을 수행할 수 있습니다. 이 릴리스에는 대상 웹 서버에서 이 취약성을 탐지하는 검사가 포함되어 있습니다.

Cross-Site Scripting: DOM[4]

Cross-Site Scripting 은 동적으로 생성된 웹 페이지가 검증되지 않은 사용자 입력(예: 로그인 정보)을 표시할 때 발생하며, 공격자가 생성된 페이지에 악성 스크립트를 삽입한 후 해당 사이트를 보는 모든 사용자의 컴퓨터에서 스크립트를 실행할 수 있도록 합니다. DOM(Document Object Model) 기반 XSS 의 경우, 악성 콘텐츠가 DOM 조작의 일환으로 실행됩니다. 공격에 성공하면 DOM Cross-Site Scripting 취약성을 악용하여 쿠키를 조작 또는 도용하거나, 유효한 사용자의 것으로 오인될 수 있는 요청을 만들거나, 기밀 정보를 손상시키거나, 최종 사용자 시스템에서 악성 코드를 실행할 수

[4] WI v21.2.0 이상이 필요합니다.

있습니다. 이 릴리스에는 클라이언트 측 URI 조각에서 DOM XSS 를 탐지하는 새로운 검사가 포함되어 있습니다.

웹 서버 구성 오류: Insecure Mapping Directives

웹 서버에서 PHP 를 실행하도록 Nginx 를 구성하는 것은 때때로 .php 로 끝나는 모든 URI 를 백엔드 PHP 인터프리터(FastCGI 등)로 전달할 수 있게 만듭니다. 이러한 안전하지 않은 PHP 구성을 가진 Nginx 는 요청된 전체 경로가 실제 존재하는 파일로 연결되지 않는 경우 URL 경로에 있는 폴더를 실행할 대상 파일로 간주합니다. 이러한 잘못된 구성으로 인해 공격자는 웹 서버에 파일을 업로드하고 액세스 가능하도록 만들 수 있는 경우 이미지 파일 등 어떠한 유형의 파일에서도 임의 PHP 코드를 실행할 수 있습니다. 이 릴리스에는 대상 웹 서버에서 이 취약성을 탐지하는 검사가 포함되어 있습니다.

Integer Overflow

0.5.6 부터 1.13.2 까지의 Nginx 버전은 CVE-2017-7529 에서 발견된 정수 오버플로에 취약합니다. 이 문제는 Nginx 범위 필터 모듈에 존재하며, 공격자가 특수하게 조작된 요청을 전송하여 잠재적으로 중요한 정보를 얻을 수 있게 해줍니다. 이 릴리스에는 대상 웹 서버에서 CVE-2017-7529 취약점을 탐지하는 검사가 포함되어 있습니다.

컴플라이언스 보고서

2021 CWE™ (Common Weakness Enumeration) Top 25

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Weaknesses(CWE Top 25)는 2019 년에 도입되었으며 SANS Top 25 를 대체합니다. 7 월에 릴리스된 2021 CWE Top 25 는 지난 2 년 동안 NVD(National Vulnerability Database)에 보고된 취약점의 빈도 및 심각도를 정규화하는 추론적 공식을 사용하여 결정되었습니다. 이번 SecureBase 업데이트에는 이와 같은 CWE 범주에 대한 매핑이 포함되어 있습니다. 이번 SecureBase 업데이트에는 CWE Top 25 로 식별되는 범주에 직접 매핑되거나, "ChildOf" 관계를 통해 Top 25 의 CWE-ID 와 관계가 설정된 CWE-ID 에 매핑되는 검사가 포함되어 있습니다.

정책 업데이트

CWE Top 25 2021

CWE Top 25 2021 관련 검사를 포함하도록 사용자 지정된 정책이 WebInspect SecureBase 의 지원되는 정책 목록에 추가되었습니다.

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.

LDAP Injection

이 릴리스에는 오탐지를 줄이고 결과의 정확도를 향상시키기 위한 향상된 LDAP Injection 검사가 포함되어 있습니다.

CyberRes Fortify Premium Content

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

2021 CWE Top 25

새로운 상관 관계를 동반하기 위해, 이 릴리스에는 2021 CWE Top 25 를 지원하는 Fortify Software Security Center 에 대한 새로운 보고서 번들이 포함되어 있으며 Premium Content 의 Fortify 고객 지원 포털에서 다운로드할 수 있습니다.

CyberRes 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 CyberRes Fortify 지원 포털에서 얻을 수 있습니다.

Fortify 기술 지원 연락처

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

SSR 연락처

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

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