Micro Focus

Fortify 소프트웨어 보안 콘텐츠

2021 업데이트 1

2021 년 3 월 26 일

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 1,038 개의 취약점 범주를 지원하며 1 백만 개 이상의 개별 API 를 지원합니다.

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

Fortify SSR(Software Security Research)은 Fortify Secure Coding Rulepacks(영어, 버전 2021.1.0), 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 816 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Micro Focus Visual COBOL 지원(버전 6)[1]

이번 릴리스에서는 Micro Focus Visual COBOL 버전 6 에 대한 지원이 추가됩니다. 구체적으로 이 릴리스에는 Micro Focus COBOL Runtime System(RTS)에 대한 지원이 포함됩니다.COBOL 에서 이미 지원되는 Path Manipulation 범주에 대한 지원이 확대되고 다음 범주가 추가로 지원됩니다.

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

Android 11

최신 버전의 Android(API 버전 30)를 지원하기 위한 지속적인 노력의 일환으로 다음 네임스페이스가 적용됩니다.

- android.accounts
- android.app
- android.database
- android.database.sqlite

사용자는 Android 응용 프로그램의 모델링 개선을 통해 일반적인 결과와 추가 *SQL Injection* 및 *Access Control: Database* 결과가 개선되는 것을 기대할 수 있습니다.

iOS 업데이트

iOS 지원을 개선하기 위한 지속적인 노력의 일환으로 새로운 Swift 규칙이 다음 클래스에 대해 추가되었습니다.

- Foundation.NSCache
- Foundation.URLFileProtection

사용자는 Data Protection 및 Privacy Violation 과 관련된 결과에 대한 개선과 기타 취약점 유형 및 프레임워크에 대한 일반적인 개선을 기대할 수 있습니다("기타 정정표 - iOS 버그 수정" 참조).

Angular 지원 업데이트(버전 11.2.3)

이번 릴리스에서는 Angular 지원이 11.2.3 으로 확대됩니다. 구체적으로, 브라우저의 사용자 제어 정보에 대한 새로운 소스가 식별됨에 따라 이전에는 트리거되지 않았던 많은 범주가 트리거될 수 있습니다.

[1] SCA 21.1 이상이 필요합니다.

Apache Commons 업데이트

Apache Commons 는 재사용 가능한 Java 구성 요소를 제공합니다. 이번 릴리스에서 SSR 은 다음 구성 요소에 대한 지원을 업데이트했습니다.

- beanutils(1.9.4)
- collections4(4.4)
- dbutils(1.7)
- fileupload(1.4)
- lang(3.11)
- math(3.6.1)
- io(2.8.0)
- text(1.9)

이 업데이트는 이러한 구성 요소를 사용하여 응용 프로그램의 모델링을 개선하고, Log Forging 및 JSON Injection 과 같은 범주에 대한 보호 기능을 식별하며, 다음과 같은 취약점 유형이 나타날 수 있는 새로운 위치를 식별합니다.

- Access Control: Database
- Denial of Service
- Insecure Randomness: User-Controlled Seed
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak(변형)

Python(버전 3.9)

최신 버전의 Python 에 지원이 업데이트되어 코어 언어 API 의 모델링이 개선됩니다.

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.

오탐지 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.

- *코드 정확성: Erroneous Class Compare*(Java 및 Kotlin 응용 프로그램)
- *Dynamic Code Evaluation: Code Injection* 문제가 Python 3 검사에서 제거됨
- *Key Management* 문제가 모든 언어에서 거짓 긍정을 제거하도록 개선됨
- *Cross-Site Scripting: DOM* 문제(jQuery 관련 문제)가 *Cross-Site Scripting: Self* 로 올바르게 분류됨(입력 상자에서 시작된 경우)
- *Password Management* 문제가 구성 파일에서 제거됨(암호가 될 수 없는 콘텐츠와 일치하는 경우)
- *Password Management* 오탐지 개선(지역화 데이터와 일치하는 경우)
- *XML External Entity Injections* 결과가 Java Spring 응용 프로그램의 관련 없는 기능에서 제거됨
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* 에서 추가 동사를 안전한 것으로 허용할 수 있음(PATCH, DELETE, PUT)

iOS 버그 수정:
분석이 개선되면서 규칙이 업데이트되었습니다. 결과적으로 다음과 같은 취약점 유형이 개선됩니다.

- Input Interception: Keyboard Extensions Allowed
- Privacy Violation: HTTP Get
- Privacy Violation: Keyboard Caching
- Privacy Violation: Screen Caching
- Privacy Violation: Shoulder Surfing

정확성을 개선하기 위해 부수적인 업데이트가 Foundation, UIKit, WebKit, HealthKit, WatchKit, MessageUI, CoreLocation, CoreData 등 여러 프레임워크에 적용되었습니다.

제거된 범주:
이번 릴리스에서는 결과의 관련성을 개선하기 위해 다음 범주가 제거되었습니다.

- Privilege Management: Android Network

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

OGNL Expression Injection: Struts 2

CVE-2019-0231 및 CVE-2020-17530 으로 식별되는 중요한 OGNL Expression Language Injection 취약점이 Struts 버전 2.0~2.5.25 에 영향을 미칩니다. 이러한 취약점의 악용은 서버의 임의 원격 코드 실행으로 이어질 수 있습니다. 이번 릴리스에는 Struts 2 를 사용하는 웹 응용 프로그램에서 이러한 취약점을 감지하는 검사 기능이 포함되어 있습니다.

WAF 감지[2]

이번 릴리스에는 "WAF 감지" 검사가 포함됩니다. 이 검사는 검사 중에 Web Application Firewall 이 감지될 경우 정보 결과에 플래그를 지정합니다. 이러한 결과는 검사 요청이 응용 프로그램에 도달하기 전에 차단되어 검사 품질이 손상되었을 수 있음을 나타냅니다.

Hacker Level Insights[2]

Hacker Level Insights 는 개발자와 보안 전문가에게 응용 프로그램의 전체 보안 상태와 관련된 컨텍스트를 제공합니다. 이번 릴리스에는 검사 중에 응용 프로그램에서 감지된 라이브러리에 플래그를 지정하는 검사가 포함되어 있습니다. 이러한 결과가 반드시 보안 취약점을 나타내는 것은 아니지만 공격자는 알려진 취약점 또는 패턴을 식별하기 위한 시도로 대개 이러한 유형의 대상에서 정찰을 수행한다는 것을 참고하시기 바랍니다.

[2] WebInspect 21.1 이상이 필요합니다.

정책 업데이트

NIST SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 관련 검사를 포함하도록 사용자 지정된 정책이 WebInspect SecureBase 의 지원되는 정책 목록에 추가되었습니다.

CWE Top 25 2020

CWE Top 25 2020 관련 검사를 포함하도록 사용자 지정된 정책이 WebInspect SecureBase 의 지원되는 정책 목록에 추가되었습니다.

DISA STIG 5.1

DISA STIG 5.1 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.

웹 캐시 감염
이번 릴리스에는 *Web Cache Poisoning: Unkeyed Headers* 에 대한 업데이트된 검사가 포함됩니다. 이제 사용자는 의심되는 사용자 지정 헤더를 캐시 키의 일부로 추가할 수 있습니다.

안전하지 않은 Spring Boot Actuator
이번 릴리스에서는 권한이 없는 사용자가 사용할 수 있는 민감한 Spring Boot Actuator 를 감지하는 검사가 업데이트되어 더 정확한 결과를 제공합니다.

XSS 개선
이번 릴리스에는 Vue 3 및 Angular JS 1.5.9 이상에 대해 개선된 XSS 공격 검사가 포함됩니다.

Micro Focus Fortify Premium Content

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

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

2021 년 3 월 26 일