Micro Focus

Fortify 소프트웨어 보안 콘텐츠

2019 업데이트 4

2019 년 12 월 13 일

Micro Focus Fortify Software Security Research 정보

Fortify Software Security Research 팀은 최첨단 연구를 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 26 개의 프로그래밍 언어에서 1,018 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) 팀은 Fortify 보안 코딩 룰팩(영어, 버전 2019.4.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능) 및 Fortify Premium Content 의 업데이트를 바로 사용할 수 있다는 점을 알려 드립니다.

Micro Focus Fortify 보안 코딩 룰팩[SCA]

이번 릴리스에서 Fortify 보안 코딩 룰팩은 26 개의 프로그래밍 언어에서 807 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Go 최초 지원[1]

Go 가 처음으로 지원됩니다. Go 는 Google™에서 설계한 정적 유형의 오픈 소스 언어로, 간단하고 안정적이며 효율적인 소프트웨어를 쉽게 개발할 수 있도록 합니다. Go 는 C 와 구문이 비슷하지만 메모리 안전 메커니즘, 가비지 수집 및 구조적 입력 기능을 제공합니다. 이 업데이트는 10 개의 핵심 표준 라이브러리 네임스페이스에 적용되며 다음 34 개의 범주를 지원합니다.

- Access Control: Database
- Command Injection
- Connection String Parameter Pollution
- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: MIME Sniffing
- Insecure Transport
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Open Redirect
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Path Manipulation
- Path Manipulation: Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- SQL Injection
- System Information Leak: External

[1] SCA v19.2.0 이상이 필요합니다.

- System Information Leak: Internal
- Weak Encryption
- Weak Encryption: Insufficient Key Size

Spring Security

Spring Security 는 추가적인 보안 계층(예: 보안 헤더)도 제공하는 인증 및 액세스 제어 프레임워크로, 세션 고정, 클릭재킹 및 교차 사이트 요청 위조와 같은 공격에 대한 추가적인 보호를 제공합니다. 또한 Spring Security 는 Spring 기반 애플리케이션 보안을 위한 실제적인 표준입니다. 이 업데이트에는 다음 21 개 범주에 대한 지원(최대 버전 5.2.1)이 포함됩니다.

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: Overly Broad Domain
- Cross-Site Request Forgery
- Header Manipulation
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Missing Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Overly Permissive Referrer-Policy
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- Session Fixation
- System Information Leak

또한 다음과 같은 7 개의 새로운 취약점 유형이 도입되었습니다.

- HTML5: Missing Framing Protection
- HTML5: Unenforced Content Security Policy
- Spring Security Misconfiguration: Default Permit
- Spring Security Misconfiguration: Disabled Security Headers
- Spring Security Misconfiguration: Incorrect Request Matcher Type
- Spring Security Misconfiguration: Lack of Fallback Check
- Spring Security Misconfiguration: Overly Permissive Firewall Policy

Spring Boot

Spring Boot 는 독립 실행형 Spring 애플리케이션을 생성하고 가능할 때마다 자동으로 Spring 및 타사 라이브러리를 구성합니다. 또한 메트릭, 상태 검사, 외부 구성 등 프로덕션에 즉시 사용할 수 있는 기능을 제공합니다. 이전에 지원된 범주와 더불어 이 업데이트에는 다음과 같은 추가 9 개 범주에 대한 지원(최대 버전 2.2.1)이 포함됩니다.

- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Overly Broad Session Cookie Domain
- Cookie Security: Overly Broad Session Cookie Path
- Cookie Security: Persistent Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Password Management: Empty Password in Configuration File

- Insecure Transport
- Insecure Transport: Server Identity Verification Disabled
- System Information Leak: External

또한 이전 룰팩은 속성 구성 파일 및 Maven 구축 시스템만 지원했지만 이번 릴리스에는 YAML 구성 파일 및 Gradle 에 대한 지원도 포함됩니다.

Java 12[2]

Java 12 의 새로운 API 를 지원합니다. 새로운 Switch 문과 같은 새로운 Java 12 구문이 사용될 경우 이러한 규칙에 SCA 버전 19.1 이상이 필요합니다.

JSTL XML 라이브러리

JSTL(JSP(JavaServer Pages) Standard Tag Library)은 JSP 중심의 XML 문서 조작 및 생성 방식을 제공하는 라이브러리입니다. JSTL v1.1 의 경우 이제 다음 범주의 지원이 포함됩니다.

- XSLT Injection
- XML External Entity Injection
- Privacy Violation
- System Information Leak: External

OpenXML SDK .NET 개선 사항

OpenXML SDK v2.9.0 에 대한 지원이 업데이트되어 다음 3 개의 추가 범주가 지원됩니다.

- Access Control: Database
- Connection String Parameter Pollution
- SQL Injection

React-Router 지원

React Router 는 애플리케이션을 선언적으로 구성하는 탐색 구성 요소 모음입니다. 웹 애플리케이션에 북마크 가능 URL 을 지정하든, React 에서 구성 가능한 탐색 방법을 지정하든 관계없이 React Router 는 React 가 렌더링되는 모든 위치에서 작동합니다. React-Router 5.1.2 에 대해 지원되는 범주에는 다음이 포함됩니다.

- Open Redirect
- Privacy Violation
- System Information Leak: External

2019 CWE Top 25

CWE(Common Weakness Enumeration) Top 25 는 SANS Top 25 로 알려졌던 때와 비교하여 Top 25 결정 방식을 근본적으로 변경했습니다. 9 월에 릴리스된 새로운 Top 25 는 지난 2 년 동안 NVD(National Vulnerability Database)에 보고된 취약점의 빈도 및 민감도를 일반화하는 추론적 공식을 사용하여 결정됩니다. NVD 에서 가장 일반적으로 보고된 치명적인 취약점을 중심으로 감사의 우선 순위를 지정하고자 하는 고객을 지원하기 위해, Micro Focus Fortify Taxonomy 와 CWE Top 25, 2019 버전 사이의 상관 관계가 추가되었습니다.

[2] SCA v19.2.0 이상이 필요합니다.

DISA STIG 4.10

컴플라이언스 영역에서 연방 고객을 지원하기 위해, Micro Focus Fortify Taxonomy 와 DISA(Defense Information Systems Agency) Application Security 및 Development STIG 버전 4.10 사이의 상관 관계가 추가되었습니다.

기타 정정표

이번 릴리스에서는 오탐지 문제의 수를 줄이고 고객이 더 쉽게 문제를 감사할 수 있도록 개선하기 위해 지속적으로 노력했습니다. 고객은 또한 다음과 관련하여 보고한 문제의 변경 사항을 확인할 수 있습니다.

- 안전하지 않은 역직렬화 일관성: 이전에는 일부 규칙에 따라 정보 출처가 브라우저인 경우에만 플래그가 지정되었습니다. 이는 다른 가능한 시나리오에서 플래그를 지정하도록 수정되었습니다.
- 설명 참조의 검증 완료: 참조된 자료의 일부가 오래되었거나 잘못된 링크를 가리켰습니다. 이러한 문제는 이제 수정되었으며 알맞은 참조가 배치되었습니다.

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

SSO Bad Practices: Authentication Token Replay

Single Sign-On 프로세스 동안 교환된 인증 토큰은 재생 공격에 취약하며 공격자가 올바른 사용자를 가장하여 서비스에 대한 무단 액세스 권한을 얻을 수 있습니다. 이번 릴리스에는 SAML 프로토콜을 사용하는 Windows ID 프레임워크 및 서비스 공급자에 대한 재생 공격을 수행하는 검사가 포함됩니다.

Cache Management: Headers

HTTP Vary 응답 헤더에는 HTTP 헤더 목록이 포함되어 있으며, 이를 바탕으로 들어오는 요청을 처리하는 캐시된 응답이 올바른지를 확인합니다. Vary 헤더에 'Origin'이 없으면 특히 교차 원본 요청이 수행될 때 애플리케이션이 클라이언트 측 및 서버 측 캐시 감염 공격을 받을 수 있습니다. 이번 릴리스에는 Vary 헤더 값에 'Origin' 헤더가 누락된 경우를 감지하는 검사가 포함됩니다.

HTML5: CORS Functionality Abuse

null 원본인 'Origin: null'에서 시작되는 CORS 요청을 허용하면 시스템 보안이 손상될 수 있으며 애플리케이션이 데이터 도난에 취약해질 수 있습니다. 이번 릴리스에는 서버 응답

내 Access-Control-Allow-Origin CORS 헤더의 'null' 값 존재를 감지하는 검사가 포함됩니다.

Insecure Deployment: HTTP Request Smuggling[3]

HTTP Request Smuggling 취약점은 프런트엔드 및 백엔드 서버에 의한 호환되지 않는 HTTP 헤더의 구문 분석 불일치로 인해 발생합니다. 공격자는 다른 서버에 의해 길이가 다른 것으로 해석되는 요청을 제공함으로써 백엔드 TCP/TLS 소켓을 감염시키고 그 다음 요청에 임의의 데이터를 추가하거나 프런트엔드 서버에서 인식하지 못한 상태로 백엔드 서버에 추가 요청을 몰래 반입할 수 있습니다. 이번 릴리스에는 이 취약점을 감지하는 검사가 포함됩니다.

Header Manipulation[4]

기존 Header Manipulation 검사는 이번 릴리스에서 기존 CRLF 공격 외에도 캐리지 리턴('CR') 및 줄 바꿈('LF') 공격을 포함하도록 개선되었습니다.

컴플라이언스 보고서

DISA STIG 4.10

컴플라이언스 영역에서 연방 고객을 지원하기 위해, 이번 릴리스에는 WebInspect 검사와 Defense Information Systems Agency Application Security 및 Development STIG 의 최신 버전인 버전 4.10 사이의 상관 관계가 포함되어 있습니다.

정책 업데이트

DISA STIG 4.10

DISA STIG 4.10 관련 검사를 포함하도록 사용자 정의된 정책이 WebInspect SecureBase 의 기존 지원 정책 목록에 추가되었습니다.

Micro Focus Fortify Premium Content

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

DISA STIG 4.10 및 2019 CWE Top 25

새로운 상관 관계를 동반하기 위해, 이번 릴리스에는 DISA STIG 4.10 과 2019 CWE Top 25 를 모두 지원하는 Fortify Software Security Center 에 대한 새로운 보고서 번들이 포함되어 있으며 이는 Premium Content 의 Fortify 고객 지원 포털에서 다운로드할 수 있습니다.

[3] Insecure Deployment: HTTP Request Smuggling 검사를 위해 WebInspect v19.2.0 이상이 필요합니다.
[4] Header Manipulation 개선 사항에는 WebInspect v19.2.0 이상이 필요합니다.

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

2019 년 12 월 13 일