Micro Focus

Fortify 소프트웨어 보안 콘텐츠

2020 업데이트 1

2020 년 3 월 27 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 26 개의 프로그래밍 언어에서 1,019 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 2020.1.0), 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 26 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.

GoLang 표준 라이브러리 지원 [1]

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 다음 19 개의 추가 범주를 비롯한 53 개의 취약점 유형을 지원합니다.

- Denial of Service: Regular Expression
- Formula Injection
- Insecure Randomness
- JSON 삽입
- 키 관리: 빈 HMAC 키
- 키 관리: 하드코딩된 HMAC 키
- 로그 위조
- 로그 위조(디버그)
- Resource Injection
- 취약한 암호화 해시
- 취약한 암호화 해시: 하드코딩된 솔트
- 취약한 암호화 해시: 사용자 제어 솔트
- 취약한 암호화 서명: 불충분한 키 크기
- 취약한 암호화 서명: 사용자 제어 키 크기

[1] 최적의 스캔 결과를 얻으려면 SCA v20.1.0 이상을 사용하는 것이 좋습니다.

- 취약한 암호화: 부적절한 RSA 패딩
- 취약한 암호화: 안전하지 않은 초기화 벡터
- 취약한 암호화: 스트림 암호
- 취약한 암호화: 사용자 제어 키 크기
- XML 삽입

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.

- JavaScript 에서 "Cross-Site Scripting: DOM"(더 정확하게는 자체 XSS 로 식별됨) 인스턴스가 새로운 하위 범주인 "Cross-Site Scripting: Self"로 변경되었으며 이제 더 낮은 우선 순위로 플래그가 지정됩니다.

- Java 에서 모델링 엔진이 개선되어 특히 if 조건과 관련하여 Dead Code 거짓 긍정 수가 의도치 않게 늘어났습니다. 그리고 규칙이 개선되어 잘못된 문제가 다수 제거되었습니다.

- 드물지만 JSP 및 Spring MVC 애플리케이션과 관련하여 발생하는 성능 문제가 해결되었습니다.

- 7 Pernicious Kingdoms 라고도 하는 Micro Focus Fortify: Software Security Errors Taxonomy 와 CWE™(Common Weakness Enumeration)의 상관 관계 개선을 위해 외부 메타데이터가 업데이트되었습니다. 구체적으로는 Software Security Errors TAxonomy 의 935 개 범주에서 CWE-ID 41 개가 추가로 정렬되어 CWE 및 CWE Top 25 2019 매핑이 모두 업데이트되었습니다. 따라서 관련 보고 기능 또는 CWE 기준 '그룹화 방법' 필터링이 영향을 받게 됩니다. 추가 CWE ID 는 다음과 같습니다.

  CWE-88, CWE-97, CWE-119, CWE-147, CWE-192, CWE-203, CWE-212, CWE-266, CWE-267, CWE-276, CWE-279, CWE-280, CWE-346, CWE-347, CWE-436, CWE-506, CWE-527, CWE-529, CWE-530, CWE-531, CWE-536, CWE-540, CWE-541, CWE-548, CWE-550, CWE-705, CWE-775, CWE-799, CWE-917, CWE-921, CWE-923, CWE-925, CWE-926, CWE-937, CWE-942, CWE-1004, CWE-1021, CWE-1069, CWE-1173,

CWE-1188, CWE-1236

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

위험 파일 포함: 로컬

Tomcat 에 영향을 주는 심각한 취약점이 AJP 프로토콜 기능을 활용하여 서버 측 파일 액세스 권한을 확보합니다. 그러면 공격자가 Apache Tomcat webapp 디렉터리에 있는 모든 파일을 읽거나 포함할 수 있습니다. 이 취약점(GhostCat)은 CVE-2020-1938 로 식별됩니다. 또한 임의 코드 실행 공격도 발생할 수 있습니다. 이 문제는 Apache Tomcat 9.x(9.0.31 이전 버전), 8.x(8.5.51 이전 버전), 7.x(7.0.100 이전 버전) 및 모든 이전 버전에 영향을 줍니다. 이번 SecureBase 업데이트에는 이 취약점을 감지하는 검사가 포함되어 있습니다.

CWE™(Common Weakness Enumeration) 매핑:

CWE™(Common Weakness Enumeration)는 소프트웨어에서 취약점 발생의 원인이 될 수 있는 소프트웨어 오류 분류입니다. 이 분류를 사용하면 SDLC 의 여러 단계 중에 수행하는 소프트웨어 위험 및 취약점 평가에 다양한 방법론에서 제공된 출력을 통합할 수 있습니다. 이번 릴리스에서 SecureBase 에는 CWE 의 최신 업데이트에 해당하는 업데이트된 검사 매핑이 포함되어 있습니다. CWE 는 계층식 분류이며, 검사는 검사 의도와 일치하는 가장 가까운 리프 노드에 매핑됩니다.

컴플라이언스 보고서

CWE™(Common Weakness Enumeration) Top 25:

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Errors(CWE Top 25)는 MITRE 에서 작성한 목록입니다. 이 목록은 소프트웨어에서

취약점 발생의 원인이 될 수 있는 가장 일반적인 소프트웨어 취약점 범주 25 가지를 제시합니다. 이번 SecureBase 업데이트에는 이와 같은 CWE 범주에 대한 매핑이 포함되어 있습니다. CWE Top 25 로 식별되는 범주에 직접 매핑되거나, "ChildOf" 관계를 통해 Top 25 의 CWE-ID 와 관계가 설정된 CWE-ID 에 매핑되는 검사가 포함되었습니다.

정책 업데이트

CWE™(Common Weakness Enumeration)

CWE™(Common Weakness Enumeration) Top 25 Most Dangerous Software Errors(CWE Top 25)는 MITRE 에서 작성한 목록입니다. 이 목록은 소프트웨어에서 취약점 발생의 원인이 될 수 있는 가장 일반적인 소프트웨어 취약점 범주 25 가지를 제시합니다. 이 릴리스에는 CWE Top 25 에 매핑된 취약점을 평가하기 위한 검사 목록이 들어 있는 정책이 포함되었습니다.

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.

- HTTP Request Smuggling 검사의 버그가 수정되어 검사 ID 가 11621 인 검사 결과와 관련된 거짓 긍정이 감소했습니다. 즉, 이 검사에서는 HTTP 405 를 유효한 취약점 확인 항목으로 더 이상 간주하지 않습니다.

- Insecure Transport: 이제 구성 문자열에 !SHA246 및 !SHA384 를 포함하는 방식을 통해 CBC 모드 암호를 제외하는 예제가 취약한 SSL 암호 보고서 콘텐츠에 포함되었습니다. 하지만 서버 관리자와 협의하여 화이트리스트로 지정된 강력한 암호 그룹을 선택해 구성을 작성하는 것이 좋습니다.

- 서버가 TLS1.2 및 강력한 암호만 지원하는 경우 검사에서 올바른 암호를 탐지할 수 없었던 상황에서 구성 탐지를 개선하기 위해 Insecure Transport: 취약한 SSL 암호 탐지가 추가로 수정되었습니다.

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. Fortify 연구팀은 이 표준의 적용 가능 요구 사항에 대한 SecureBase 검사 및 SCA 규칙의 매핑을 작성했습니다. 그런데 제품과의 상관 관계 작성 과정에서 SecureBase 검사 및 SCA 규칙과 더 정확하게 일치하도록 표준이 제공하는 CWE 매핑을 개선할 수 있는 경우가 확인되었습니다. 이러한 매핑을 개선하면서 관심이 있는 고객에게 평가 및 공동 작업용으로 해당 아티팩트를 제공해 드릴 수 있습니다. 관심이 있으신 경우 아래의 SSR 연락처로 문의해 주시면 WebInspect 용 컴플라이언스 템플릿과 정책 또는 SSC 시드 번들을 받으실 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 해당 업데이트를 받을 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

2020 년 3 월 27 일

errors or omissions contained herein.