Micro Focus

Fortify 소프트웨어 보안 콘텐츠

2020 업데이트 4

2020 년 12 월 18 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 1,039 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 2020.4.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능) 및 Fortify Premium Content 의 업데이트를 바로 사용할 수 있다는 점을 알려 드립니다.

Micro Focus Fortify Secure Coding Rulepacks[SCA]

이 릴리스에서 Fortify Secure Coding Rulepacks 는 27 개의 프로그래밍 언어에서 817 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Dapper 지원(버전 2.0.78)

Dapper ORM(Object-Relational Mapping)을 지원합니다. Dapper 는 NET IDdbConnection 인터페이스를 확장하여 네이티브 쿼리 출력을 강력한 형식의 C# 개체에 매핑하는 데 사용됩니다. 새로운 지원에서는 Dapper 를 사용자 제어 데이터의 소스이자 다음과 같은 범주의 트리거로 취급합니다.

- Access Control: Database
- SQL Injection

Kotlin 표준 라이브러리 업데이트(버전 1.3)

다음 패키지의 적용 범위를 포함하도록 Kotlin 표준 라이브러리에 대한 지원이 확장되었습니다.

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull(버전 1)

Android 의 XML Pull 패키지 구현을 지원합니다. XML Pull 은 XML 파일을 구문 분석하고 직렬화하는 데 사용되는 간단한 스트리밍 API 이며, 응용 프로그램이 구문 분석을 제어합니다(중단 및 재개 가능). 지원되는 범주는 다음과 같습니다.

- XML Entity Expansion Injection
- XML 삽입

AIOPG(버전 1.0.0)[1]

Python aiopg 라이브러리를 지원합니다. Aiopg 는 PostgreSQL 데이터베이스에 연결하는 비동기 방식을 제공합니다. 지원되는 범주는 다음과 같습니다.

- Access Control: Database
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- SQL Injection

JavaScript Promises

- 데이터 흐름 분석을 위해 JavaScript Promises 에 대한 지원이 개선되었습니다.

Azure Resource Management 템플릿

ARM(Azure Resource Management) 템플릿에 대한 초기 지원입니다. ARM 템플릿은 Azure 솔루션용 코드로 인프라를 구현하는 데 사용됩니다. ARM 템플릿은 선언적 구문을 사용하여 사용자의 프로젝트를 정의하고 구성하는 JSON 파일입니다. 지원되는 범주는 다음과 같습니다.

- Azure Resource Manager 구성 오류: HTTPS 를 요구하지 않음
- Azure Resource Manager 구성 오류: 공개 액세스 허용됨

DISA STIG 5.1

컴플라이언스 영역에서 연방 고객을 지원하기 위해, Micro Focus Fortify Taxonomy 와 DISA(Defense Information Systems Agency) Application Security 및 Development STIG 버전 5.1 사이의 상관 관계가 추가되었습니다.

NIST SP 800-53 Rev. 5

컴플라이언스 영역에서 연방 고객을 지원하기 위해 Micro Focus Fortify Taxonomy 와 NIST(National Institute of Standards and Technology) SP(Special Publication) 800-53 개정

[1] aiopg 와 관련된 문제의 완전한 감지는 'async with'와 관련된 SCA 의 향후 개선에 달려 있습니다.

5 의 최신 버전에 설명된 보안 및 개인정보 제어 사이의 상관 관계가 추가되었습니다. 다음 제어 제품군에 대한 30 개 기본 제어에 적용됩니다.

- AC(Access Control: 액세스 제어)
- AU(Audit and Accountability: 감사 및 책임)
- CA(Assessment, Authorization, and Monitoring: 평가, 인증 및 모니터링)
- CM(Configuration Management: 구성 관리)
- IA(Identification and Authentication: 식별 및 인증)
- PT(PII Processing and Transparency: PII 처리 및 투명성)
- SC(System and Communications Protection: 시스템 및 통신 보호)
- SI(System and Information Integrity: 시스템 및 정보 무결성)

2020 CWE™(Common Weakness Enumeration) Top 25

CWE™(Common Weakness Enumeration) Top 25 는 2019 년에 도입되었으며 SANS Top 25 를 대체합니다. 8 월에 릴리스된 2020 CWE Top 25 는 지난 2 년 동안 NVD(National Vulnerability Database)에 보고된 취약점의 빈도 및 심각도를 정규화하는 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 2020 CWE Top 25 사이의 상관 관계가 추가되었습니다.

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.

17.x 이전 SCA 버전의 사용 중단

2020.3 릴리스 발표에서 언급했듯이, 해당 릴리스는 17.x 이전의 SCA 버전을 지원하는 규칙 팩의 마지막 릴리스였습니다. 이 릴리스에서는 17.x 이전 SCA 버전에서 최신 규칙 팩이 로드되지 않습니다. 17.x 이전 SCA 버전을 사용하는 고객은 규칙 팩을 다운그레이드하거나 SCA 버전을 업그레이드해야 합니다.

향후 릴리스에서는 SCA 의 마지막 4 가지 주 릴리스가 지원됩니다.

매핑 폐기

Software Security Research 팀은 수년에 걸쳐 Fortify 범주를 외부 표준 및 모범 사례에 연결하는 매핑을 작성해왔습니다. 이제 지원되는 표준의 서로 다른 버전이 매우 크게 증가하는 지점에 이르렀지만 많은 수의 이전 버전은 앞으로 사용되지 않을 것입니다.

이러한 이유로 이제 다음과 같은 표준을 "obsolete"(폐기)로 표기합니다.

- PCI(지불 카드 업계 데이터 보안 표준) 1.1
- PCI(지불 카드 업계 데이터 보안 표준) 1.2
- PCI(지불 카드 업계 데이터 보안 표준) 2.0

- PCI(지불 카드 업계 데이터 보안 표준) 3.0
- PCI(지불 카드 업계 데이터 보안 표준) 3.1
- PCI(지불 카드 업계 데이터 보안 표준) 3.2
- STIG(보안 기술 구현 가이드) 4.1
- STIG(보안 기술 구현 가이드) 4.2
- STIG(보안 기술 구현 가이드) 4.3
- STIG(보안 기술 구현 가이드) 4.4
- STIG(보안 기술 구현 가이드) 4.5
- STIG(보안 기술 구현 가이드) 4.6
- STIG(보안 기술 구현 가이드) 4.7
- STIG(보안 기술 구현 가이드) 4.8

이 변경 사항으로 인해 Fortify SCA 응용 프로그램 버전 20.2 이상에서 기본적으로 이러한 이전 매핑이 표시되지 않습니다.

이러한 이전 버전의 컴플라이언스를 확인해야 하는 경우 *obsolete* 특성을 "false"로 설정하도록 매핑을 변경하거나 특성을 완전히 제거해야 합니다.

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.

- 구성 파일에 보호가 있는 경우 HTTP Verb Tampering(HTTP 동사 변조) 거짓 긍정을 제거했습니다.
- .NET 에서 JSONIGNORE 특성을 사용할 경우 Mass Assignment(대량 할당) 거짓 긍정을 제거했습니다.
- URLSessionConfiguration 개체에서 캐시가 명시적으로 비활성화된 경우 Insecure Storage: HTTP Response Cache Leak(안전하지 않은 저장소: HTTP 응답 캐시 누출) 거짓 긍정을 제거했습니다.
- URLRequest 에서 Swift Privacy Violation: Http Get(Swift 개인정보 위반: Http Get) 거짓 긍정을 제거했습니다.
- 취약한 로깅 관행: 시스템 출력 스트림 사용 중복이 Python 에서 제거되었습니다.

- 추가적인 Apache Commons closeQuietly 변형 사용 시 릴리스되지 않은 리소스 문제가 제거되었습니다.

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

취약한 암호화 서명: 예측 가능한 비밀 키

JSON Web Token 페이로드 무결성은 종종 HMAC 서명을 사용하여 보장됩니다. 그러나 HMAC 알고리즘이 약한 암호를 사용하는 경우 악의적인 사용자가 무차별 대입 공격으로 비밀 키를 얻고 페이로드로 JWT 에 다시 서명할 수 있습니다. 이 릴리스에는 일반적으로 사용되는 암호의 문자열이 JWT 토큰 서명에 사용되는지 여부를 확인하는 검사가 포함됩니다.

Password Management: 취약한 암호 정책

사용자가 강력한 암호를 생성할 수 있도록 확인하는 암호 정책은 안전한 웹 사이트를 배포하는 데 매우 중요합니다. 암호 유효성을 검사하여 암호가 일반적으로 사용되는 암호 중 하나가 아니며 암호 문자열이 NIST 800-53, NIST 800118 및 OWASP 에 설정된 지침을 충족하는지 확인해야 합니다. 이 릴리스에는 로그인 매크로에 구성된 암호가 일반적으로 사용되는 암호 중 하나와 일치하는지 여부를 감지하는 새로운 검사가 포함되어 있습니다. 또한 이 릴리스에는 위에서 언급한 NIST 표준 및 OWASP 지침에 설정된 암호 강도에 대한 수정된 지침을 충족하기 위해 취약한 암호 정책 검사에 대한 업데이트가 포함되어 있습니다.

Cache Management: 웹 캐시 감염

웹 캐시는 사용자가 웹 사이트를 처음 방문할 때 페이지 사본을 저장합니다. 다음번에 사용자가 동일한 페이지를 방문하면 캐시된 사본이 제공됩니다. 그러나 이러한 웹 캐시에 요청 본문(예: fat GET 요청 또는 키가 지정되지 않은 입력)을 포함하는 GET 요청을 수락하는 것과 같은 구현 또는 설계 결함이 있는 경우 웹 캐시 감염에 취약할 수 있습니다. 웹 캐시 감염은 공격자가 합법적인 사용자 요청에 대해 악성 응답을 캐시하기 위해 사용하는 고급 기술입니다. 이 릴리스에는 키가 지정되지 않은 헤더 및 fat GET 요청을 통한 웹 캐시 감염에 웹 사이트가 취약한지 여부를 확인하는 검사가 포함되어 있습니다.

컴플라이언스 보고서

DISA STIG 5.1

컴플라이언스 영역에서 연방 정부 고객을 지원하기 위해, 이번 릴리스에는 WebInspect 검사와 Defense Information Systems Agency Application Security 및 Development STIG 의 최신 버전인 버전 5.1 사이의 상관 관계가 포함됩니다.

NIST SP 800-53 Rev. 5

컴플라이언스 영역에서 연방 정부 고객을 지원하기 위해, 이번 릴리스에는 WebInspect 검사와 NIST(National Institute of Standards and Technology) SP(Special Publication) 800-53 개정 5 의 최신 버전 간 상관 관계가 포함됩니다.

2020 CWE™(Common Weakness Enumeration) Top 25

CWE™(Common Weakness Enumeration) Top 25 는 2019 년에 도입되었으며 SANS Top 25 를 대체합니다. 8 월에 릴리스된 2020 CWE Top 25 는 지난 2 년 동안 NVD(National Vulnerability Database)에 보고된 취약점의 빈도 및 심각도를 정규화하는 추론적 공식을 사용하여 결정됩니다. 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 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.

- HTTP Request Smuggling 검사는 거짓 긍정을 줄이고 효율성을 높이며 결과의 정확성을 높이기 위해 재설계되었습니다. 검사 ID 11621 은 더 이상 취약성 확인을 위해 시간 기반 접근 방식을 사용하지 않습니다.

Micro Focus Fortify Premium Content

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

DISA STIG 5.1, NIST SP 800-53 개정 5 및 2020 CWE Top 25

새로운 상관 관계를 동반하기 위해, 이번 릴리스에는 DISA STIG 5.1, NIST SP 800-53 개정 5 및 2020 CWE Top 25 를 지원하는 Fortify Software Security Center 에 대한 새로운 보고서 번들이 포함되어 있으며 이는 Premium Content 의 Fortify 고객 지원 포털에서 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

2020 년 12 월 18 일

2020 년 12 월 18 일