Micro Focus

Fortify 소프트웨어 보안 콘텐트

2019 업데이트 1

2019 년 3 월 29 일

Micro Focus Fortify Software Security Research 정보

Fortify 소프트웨어 보안 연구팀은 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 콘텐트는 25 개의 프로그래밍 언어에서 999 개의 취약점 범주를지원하며 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 2019.1.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능), Fortify Application Defender 및 Fortify Premium Content 의 업데이트를 바로 사용할 수 있다는 점을 알려 드리게 되어 기쁘게 생각합니다.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

이 릴리스에서 Fortify Secure Coding Rulepacks 는 25 개의 프로그래밍 언어에서 796 가지 고유 범주의 취약점을 감지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 요약하면 이 릴리스에는 다음 사항이 포함됩니다.

Angular 7[1]

7.0.0 이하의 버전 지원을 포함하여 Angular 지원은 브라우저에서 입력 소스를 식별하고 기본적으로 Angular 로 수행되는 보안 검증을 모델링합니다. Angular 템플릿은 DOM, Privacy Violation, Dynamic Code Evaluation 문제 등을 비롯한 Cross-Site Scripting 과 같은 범주를 찾는 기능을 포함하여 Angular 프로젝트에서 모든 일반 JavaScript 싱크를 지원하도록 모델링됩니다.

AWS Lambda 함수 지원

새로운 AWS(Amazon Web Services) Lambda 함수는 Java 및 Python 언어를 지원합니다. 이 기능을 통해 Lambda 가 API 게이트웨이에 연결될 때 발생할 수 있는 XSS 문제를 포함하여 Lambda 트리거 이벤트에서 Lambda 함수 논리로의 데이터 흐름이 가능합니다.

AWS Java SDK v2

S3 및 DynamoDB 서비스용 AWS Java SDK v2 가 새롭게 지원됩니다. 포함되는 새 범주는 다음과 같습니다.

- Access Control: ACL Manipulation
- Insecure Storage: S3 Full Anonymous Access
- Insecure Storage: S3 Read ACP Anonymous Access
- Insecure Storage: S3 Read Anonymous Access
- Insecure Storage: S3 Write Anonymous Access
- Insecure Storage: S3 Write ACP Anonymous Access
- NoSQL Injection: DynamoDB

Python Django[1]

최대 2.1.7 버전의 지원을 포함하여 Python Django Web Framework 에 대한 지원이 업데이트되었습니다. Django 1.8 이후 도입된 Django 함수/메서드에 대한 지원뿐 아니라 클래스 기반 보기 및 관련 데이터 흐름의 지원이 향상되도록 변경되었습니다.

Apache Wicket[1]

Framework 버전 6, 7 및 8 지원을 포함하여 Apache Wicket Web Framework 에 대한 지원이 개선되었습니다.

[1] Angular 7, Django 및 Wicket 을 지원하는 데 있어 최적의 결과를 얻으려면 Fortify SCA 버전 19.1.0 이상이 필요합니다.

DISA STIG 4.9

컴플라이언스 영역에서 연방 고객을 지원하기 위해, Micro Focus Fortify Taxonomy 와 Defense Information Systems Agency(DISA) Application Security 및 Development STIG 버전 4.9 사이의 상관 관계가 추가되었습니다.

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

Often Misused: 파일 업로드

Blueimp 의 jQuery File Upload 위젯은 CVE-2018-9206 으로 식별된 원격 코드 실행에 취약한 것으로 밝혀졌습니다. 이 취약점으로 인해 공격자는 임의의 PHP 파일을 업로드하고 실행할 수 있습니다. 이 릴리스는 이 취약점을 감지하는 검사를 포함합니다.

SQL Injection

이 릴리스에서는 Microsoft Azure SQL 데이터베이스를 사용하는 응용 프로그램에 대한 지원을 포함하도록 SQL Injection 검사가 향상되었습니다.

Sensitive Information Leak: External

이 릴리스에는 Magento CMS 가 개발자 모드에서 실행 중인지를 감지하는 검사가 포함되어 있습니다. 개발자 모드는 개발 또는 테스트 환경에서 사용하기 위한 것입니다. 운영 환경에서 개발자 모드를 활성화하면 잠재적인 공격자에게 중요한 응용 프로그램 및 시스템 데이터가 노출되어 보안 위험이 발생할 수 있습니다.

Cross-Frame Scripting

콘텐트 보안 정책 *frame-ancestors* 지시문 헤더는 Cross-Frame Scripting 취약점에 대한 정책 보호 기능을 제공합니다. 현재 사용되고 있는 X-Frame-Options HTTP 헤더는 더 이상 사용되지 않습니다. 이 릴리스에서는 콘텐트 보안 정책 frame-ancestors 지시문을 지원할 수 있도록 기존 Cross-Frame Scripting 검사에 대한 기능이 향상되었습니다.

CMS(Content Management System) 지문 인식

이 릴리스에는 WebInspect 검사 중에 대상 서버에 다음 CMS 중 하나의 존재 여부에 대한 지문 인식 기능이 포함되어 있습니다. CMS 로는 WordPress, Drupal, Django, Joomla,

Liferay, Magento, Sitecore, Sitefinity[2] 및 Umbraco 가 있습니다. 검사 결과를 보고하도록 정보 검사가 트리거됩니다.

컴플라이언스 보고서

DISA STIG 4.9

컴플라이언스 영역에서 연방 고객을 지원하기 위해, 이 릴리스에는 WebInspect 검사와 Defense Information Systems Agency Application Security 및 Development STIG 의 최신 버전인 버전 4.9 사이의 상관 관계가 포함되어 있습니다.

정책 업데이트

DISA STIG 4.9

DISA STIG 4.9 관련 검사를 포함하도록 사용자 정의된 정책이 WebInspect SecureBase 의 기존 지원 정책 목록에 추가되었습니다.

Micro Focus Fortify Application Defender

Fortify Application Defender 는 조직이 자체 또는 타사 애플리케이션의 위험을 관리 및 경감하는 데 도움을 주는 RASP(Runtime Application Self-Protection) 솔루션입니다. 실시간으로 응용 프로그램 사용 및 악용에 대한 중앙 집중식 가시성을 제공하는 동시에 소프트웨어 취약성 악용 및 기타 위반으로부터 시스템을 보호합니다. Micro Focus Fortify Software Security Research 팀은 이 릴리스에서 다음과 같이 향상된 기능을 제공합니다.

OGNL 식 삽입: Struts 2

CVE-2018-11776 으로 식별된 심각한 Struts 취약점을 다루는 Apache Struts 2 의 OGNL Injection 감지에 대한 지원이 확대되었습니다. Apache Struts2 버전 2.3.x~2.3.34 또는 버전 2.5.x~2.5.16 을 사용하는 응용 프로그램에 네임스페이스 없이 구성되거나 와일드카드 네임스페이스로 구성된 작업 결과가 포함되고 struts.mapper.alwaysSelectFullNamespace 속성이 struts 구성에서 true 로 설정된 경우 공격자가 임의 OGNL 식을 실행할 수 있습니다.

Micro Focus Fortify Premium Content

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

DISA STIG 4.9[3]

[2] Sitefinity 감지에는 WebInspect 19.1.0 이상이 필요합니다.

새로운 상관 관계를 동반하기 위해, 이 릴리스에는 DISA STIG 4.9 을 지원하는 Fortify SSC 에 대한 새로운 보고서 번들이 포함되어 있으며 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 지원된 업데이트가 있는 기존 사이트를 찾는 고객은 Micro Focus Fortify 지원 포털에서 얻을 수 있습니다.

[3] DISA STIG 4.9 보고서를 지원하려면 Fortify SSC 버전 18.20 이상이 필요합니다.

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 3 월 29 일