Micro Focus

Fortify 소프트웨어 보안 콘텐츠

2018 업데이트 4

14.12.18

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 콘텐츠는 25 개의 프로그래밍 언어에서 992 개의 취약점 범주를지원하며 1 백만 개 이상의 개별 API 를 지원합니다.

자세한 내용:

https://software.microfocus.com/en-us/software/security-research

Fortify Software Security Research(SSR)는 Fortify Secure Coding Rule Pack(영어, 버전 2018.4.0), Fortify WebInspect SecureBase(SmartUpdate 를 통해 사용 가능), Fortify Application Defender 및 Fortify Premium Content 에 대한 업데이트를 즉시 이용할 수 있음을 알려드립니다.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

는 릴리스에서 Fortify Secure Coding Rulepacks 은 25 개의 프로그래밍 언어에서 789 가지 고유 범주의 취약점을 탐지하고 1 백만 개가 넘는 개별 API 를 지원합니다. 요약하면 이 릴리스에는 다음 사항이 포함됩니다.

SQLite 및 iOS 개선 사항

Swift, Objective-C, C 및 C++ 전반에 대한 SQLite API 지원이 확장되어 SQL Injection, Access Control: Database 등 16 개 기존 취약성 범주와 암호 및 키 관리 둘 다와 관련된 문제를 지원합니다. 모든 유형의 데이터베이스 상호 작용과 관련된 코딩 취약점은 중요한 정보의 누출, 의도하지 않은 수정 또는 데이터 손실을 초래할 수 있습니다. 또한 Swift 에 대한 Privacy Violation: Heap Inspection 범위를 포함하는 개인정보와 관련된 추가적인 iOS 개선이 이루어졌습니다.

Akka HTTP

전체 서버 및 클라이언트 측 HTTP 스택을 구현하는 Akka Streams 를 기반으로하는 Reactive Streams 호환 툴킷인 Scala Akka HTTP 모듈을 지원합니다. 취약성 카테고리 범위는 22 개의 기존 취약점 유형을 포함합니다.

JAX-RS 개선 사항

최신 버전의 JAX-RS 및 참조 구현 저지에 대한 지원 개정. 2.1 에 추가된 새로운 기능을 지원하는 것 외에도, 이 룰팩은 클라이언트 측 API 에 대한 지원을 포함합니다. 영향을 받는 취약점 범주에는 Privacy Violation, Server-Side Request Forgery 및 System Information Leak 가 포함됩니다. 또한 XSS 안전 콘텐츠 유형을 사용하여 응답이 전송될 때 발생하는 Cross-Site Scripting 의 특수 하위 카테고리에 대해 새로운 약점 카테고리가 추가되었습니다. 이런 경우, 이 경우 특정 브라우저가 "콘텐츠 스니핑"을 수행하고 응답에서 스크립트를 실행할 수 있으므로 "Cross-Site Scripting: Content Sniffing" 문제를 보고합니다.

Python six

"six" Python 라이브러리를 지원합니다. Six 는 수정 없이 Python 2 와 3 둘 다와 호환되는 코드베이스를 지원하기 위한 Python 호환성 라이브러리입니다. 지원되는 취약성 카테고리:

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak: External
- Unsafe Reflection

DISA STIG 4.8

컴플라이언스 영역에서 연방 고객을 지원하기 위해, Micro Focus Fortify Taxonomy 와 Defense Information Systems Agency (DISA) Application Security 및 Development STIG 버전 4.8 사이의 상관 관계가 추가되었습니다.

PCI DSS 3.2.1

컴플라이언스 영역에서 전자 상거래 및 금융 서비스 고객을 지원하기 위해, 이 릴리스에서는 Security Fortify Taxonomy 카테고리와 Payment Card Industry Data Security Standard 의 최신 버전인 버전 3.2.1 에 지정된 요구 사항 간의 상관 관계를 지원합니다.

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

LDAP Injection

LDAP Injection 은 사용자 입력을 기반으로 LDAP 구문을 구성하는 웹 기반 응용 프로그램을 악용하는 데 사용되는 공격입니다. 응용 프로그램이 사용자 입력을 적절히 무해화하지 못하면 SQL Injection 과 유사한 기술을 통해 LDAP 구문을 수정할 수 있습니다. LDAP Injection 공격은 중요한 데이터에 무단으로 액세스할 수 있습니다. 이 릴리스에는 웹 응용 프로그램의 LDAP Injection 취약점을 확인하는 검사가 포함되어 있습니다.

Open Redirect

Open Redirect 취약점은 공격자가 알려진 사이트에서 사용자의 신뢰를 쉽게 악용할 수 있게 합니다. 공급 업체 자문 SA-CORE-2018-006 에 따르면 Drupal 7 과 8 은 이 약점에 취약합니다.

Drupal Destination Parameter Anonymous Open Redirect

Drupal 8 에서, "대상" 매개 변수 값의 부적절한 무효화 처리가 악용되어 공격자가 제어하는 악의적인 URL 로 공개 리디렉션을 트리거합니다. 이 릴리스는 이 취약점을 감지하는 검사를 포함합니다.

Drupal Path Alias Open Redirect

Drupal 7 과 Drupal 8 에서, 경로 모듈의 취약점으로 인해 공격자가 경로 별칭을 작성, 편집 및 관리하여 공격자가 제어하는 악의적인 URL 로 공개 리디렉션을 트리거할 수 있습니다.

Access Control: Authorization Bypass

JSON Web Token(JWT)은 양측 간 데이터를 전송하는 URL 안전 수단을 만드는 표준입니다. 토큰 내 정보는 HMAC 또는 RSA 알고리즘을 사용하여 디지털로 서명됩니다. 하지만, 이 표준에서는 JWT 의 해시 알고리즘으로 "none"을 사용할 수도 있습니다. "none"으로 인코딩된 JWT 를 승인하는 서버는 데이터 무결성에 대한 검증을 수행하지 않고 모든 JWT 가 유효하다고 간주합니다. 악의적인 사용자는 이를 악용하여 서버에 임의의 데이터를 전송할 수 있습니다. 이로 인해 시스템 및 사용자 데이터에 대한 무단 액세스 및 손상이 발생할 수 있습니다. 이 릴리스에는 JWT "none" 알고리즘 인증 우회 취약점을 탐지하는 검사가 포함되어 있습니다.

Privacy Violation

JSON Web Token(JWT)은 양측 간에 데이터를 전송하는 데 사용됩니다. 민감한 데이터는 적절하게 암호화하지 않으면 권한이 없는 사용자에게 노출될 수 있습니다. 이 릴리스에는 신용카드 번호 공개, 사회 보장 번호 공개 및 HTML5 클라이언트 측 저장 장치 내 민감한 정보의 저장을 감지하는 것과 관련된 개인정보 위반을 탐지하는 기존 검사에 대한 업데이트가 포함되어 있습니다.

Dynamic Code Evaluation: Code Injection

Pivotal 의 Spring Framework 는 CVE-2018-1270 에 명시된 원격 코드 실행 취약점에 취약한 것으로 밝혀졌습니다.공격자가 이 취약점을 이용해 원격 코드 실행을 초래할 수 있는 WebSocket 엔드포인트를 통해 노출된 STOMP 에 악성 메시지를 보낼 수 있습니다. 이 릴리스는 Spring Framework 에서 이 취약점을 감지하는 검사를 포함합니다. 이 검사는 WebSocket 정책을 통해 액세스할 수 있습니다.

WebSocket Discovered

이 릴리스에는 스캔된 응용 프로그램에 WebSocket 이 있음을 표시하기 위한 정보 검사가 포함되어 있습니다. 또한 이 검사는 고객이 WebSocket 취약점과 관련된 모든 검사를 포함하는 새로운 WebSocket 정책으로 응용 프로그램을 스캔하도록 고려해야 함을 알립니다.

컴플라이언스 보고서

DISA STIG 4.8

컴플라이언스 영역에서 연방 고객을 지원하기 위해, 이 릴리스에는 WebInspect 검사와 Defense Information Systems Agency Application Security 및 Development STIG 의 최신 버전인 버전 4.8 사이의 상관 관계가 포함되어 있습니다.

PCI DSS 3.2.1

이 릴리스에는 최신 버전의 결제 카드 업계 데이터 보안 표준(DSS) 준수 템플릿 버전 3.2.1 에 대한 지원이 포함됩니다.

정책 업데이트

DISA STIG 4.8

DISA STIG 4.8 관련 검사를 포함하도록 사용자 정의된 정책이 WebInspect SecureBase 의 기존 지원 정책 목록에 추가되었습니다.

WebSocket

새로운 WebSocket 정책은 WebSocket 관련 취약점에 대한 응용 프로그램의 보안 평가를 수행합니다.

Micro Focus Fortify Premium Content

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

DISA STIG 4.8[1]

새로운 상관 관계를 동반하기 위해, 이 릴리스에는 DISA STIG 4.8 을 지원하는 Fortify SSC 에 대한 새로운 보고서 번들이 포함되어 있으며 Premium Content 의 Fortify 고객 지원 포털에서 다운로드할 수 있습니다.

PCI DSS 3.2.1[1]

새로운 상관 관계를 동반하기 위해, 이 릴리스에는 PCI DSS 3.2.1 을 지원하는 Fortify SSC 에 대한 새로운 보고서 번들이 포함되어 있으며 Premium Content 의 Fortify 고객 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 업데이트로 기존 사이트를 찾는 고객은 Micro Focus Fortify 지원 포털에서 얻을 수 있습니다.

[1] DISA STIG 4.8 및 PCI DSS 3.2.1 보고서에 대한 지원에는 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

2018 년 12 월 14 일