Software Security Research 릴리스 발표

Fortify 소프트웨어 보안 콘텐츠

2022 업데이트 1

2022년 3월 25일 금요일

CyberRes 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 Defender를 포함한 Fortify 제품 포트폴리오를 강화합니다. 현재 CyberRes Fortify 소프트웨어 보안 콘텐츠는 29개의 언어에서 1,166개의 취약점 범주를 지원하며 1백만 개 이상의 개별 API를 지원합니다.

CyberRes
A Micro Focus Line of Business

Fortify SSR(Software Security Research)은 Fortify Secure Coding Rulepacks(영어, 버전 2022.1.0), Fortify WebInspect SecureBase(SmartUpdate를 통해 사용 가능) 및 Fortify Premium Content의 업데이트를 바로 사용할 수 있다는 점을 알려 드립니다.

CyberRes Fortify Secure Coding Rulepacks[SCA]

이 릴리스에서 Fortify Secure Coding Rulepacks는 29개의 프로그래밍 언어에서 946가지 고유 범주의 취약점을 탐지하고 1백만 개가 넘는 개별 API를 지원합니다. 이번 릴리스에 포함되는 사항을 간략히 정리하면 다음과 같습니다.

Log4j 업데이트(지원되는 버전: 2.17)

Log4j는 프레임워크 내에서 발견된 주요 취약점으로 인해 최근 몇 달 동안 정밀 조사를 받은 널리 사용되는 Java용 로깅 프레임워크입니다. 이 릴리스에는 소스 코드의 어떤 부분이 Log4Shell 취약점에 노출되기 쉬운지 정확히 식별하고 이를 다음 범주로 플래그를 지정할 수 있도록 향상된 지원이 포함됩니다. *Dynamic Code Evaluation: JNDI Reference Injection.*
또한 업그레이드된 Log4j 지원에는 다음 네임스페이스에 대한 최신 버전의 Log4j가 포함됩니다.

- org.apache.logging.log4j

이 지원은 다음과 같은 취약점 범주에 대한 적용 범위를 개선합니다.

- Code Correctness: Stack Exhaustion
- Dynamic Code Evaluation: JNDI Reference Injection
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak

Azure Functions(Python, 지원되는 버전: 3.10.x)

Azure Functions는 API 호출, 데이터베이스 트랜잭션과 같은 미리 정의된 이벤트에 대한 응답으로 코드를 실행하거나 다른 Azure 서비스의 메시지 대기열을 관리할 수 있는 서버리스 클라우드 컴퓨팅 솔루션입니다. 이 릴리스에서는 Python의 HTTP 트리거 기능을 지원하기 위해 Azure Functions에 대한 지원을 확장했습니다. HTTP 트리거는 HTTP 요청으로 함수를 호출하는 데 도움이 되며 서버리스 API를 빌드하고 웹후크에 응답하는 데 사용할 수 있습니다.
이 지원이 적용되는 범주는 다음과 같습니다.

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- Privacy Violation
- System Information Leak: External

GraphQL 지원: Python Graphene(지원되는 버전: 3.0.0)

이 릴리스에는 Python Graphene에 대한 초기 GraphQL 서버 지원이 포함됩니다. GraphQL은 Facebook에서 개발한 오픈 소스 프로젝트로, 강력한 형식의 쿼리 언어와 API용 서버 측 런타임 엔진을 특징으로 합니다. GraphQL은 2015년부터 공개 표준이었으며 현재 24개 이상의 프로그래밍 언어에서 지원됩니다. Graphene은 Python 애플리케이션을 위한 널리 사용되는 GraphQL 서버 프레임워크입니다. 이 릴리스에서는 Graphene으로 개발한 GraphQL API의 취약점을 감지하기 위해 다음 두 가지 범주를 추가했습니다.

- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled

Kotlin 업데이트(지원되는 버전: 1.5)

Kotlin은 Java 상호 운용성을 갖춘 정적 유형의 범용 언어입니다. 이 릴리스에는 JVM(Java Virtual Machine)을 대상으로 Kotlin 1.5에 도입된 표준 라이브러리 API에 대한 업데이트된 지원이 포함됩니다.

Sequelize(지원되는 버전: 6.17)

Sequelize는 Node.js 애플리케이션 내에서 널리 사용되는 수많은 SQL 언어를 사용하는 작업을 단순화하도록 설계된 Promise 기반 ORM(개체-관계 매핑) 도구입니다. 이 지원이 적용되는 범주는 다음과 같습니다.

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

HTML의 안전하지 않은 참조 파일

웹 페이지 내의 타사 사이트에 대한 모든 참조는 보안 연결을 통해 이루어져야 합니다. 이에 따라 이 릴리스에는 HTML 파일 내 다음과 같은 새로운 범주에 대한 지원이 포함됩니다.

- Dynamic Code Evaluation: Insecure Transport
- Insecure Transport: External Link

공유 암호 데이터베이스 감지

암호 데이터베이스는 암호를 안전하게 저장하기 위해 만들어진 파일 또는 파일 집합입니다. 암호 데이터베이스는 일반적으로 마스터 암호 또는 마스터 키를 사용하여 암호화됩니다. 그러나 암호 데이터베이스를 개발 수명 주기 동안 애플리케이션 내에서 암호 사용을 지속하는 데 사용해서는 안 됩니다. 이 릴리스에서는 이러한 데이터베이스를 다음과 같이 보고합니다. *Password Management: Shared Password Database.* 지원되는 암호 데이터베이스는 다음과 같습니다.

- KeePass
- 1Password
- Password Safe
- MacOS Keychain
- Gnome Keyring
- KDE KWallet

클라우드 IaC

이 릴리스에는 클라우드 IaC(Infrastructure as Code)에 대한 확장된 지원이 포함됩니다. IaC는 수동 프로세스 대신 코드를 통해 컴퓨터 리소스를 관리하고 프로비저닝하는 프로세스입니다. AWS, AWS CloudFormation, Azure ARM, Kubernetes K8S, Azure Kubernetes Service 등의 기술을 지원합니다. 언급된 서비스 구성과 관련된 일반적인 문제는 이제 개발자에게 보고됩니다.

지원되는 추가 범주는 다음과 같습니다.

- Ansible Bad Practices: CloudWatch Log Group Retention Unspecified
- Ansible Bad Practices: Unrestricted AWS Lambda Principal
- Ansible Bad Practices: User-Bound AWS IAM Policy
- Ansible Misconfiguration: Azure Monitor Missing Administrative Events
- Insecure Storage: Missing EC2 AMI Encryption
- Insecure Storage: Missing EFS Encryption
- Insecure Storage: Missing Kinesis Stream Encryption
- Insecure Transport: Azure App Service
- Insecure Transport: Azure Storage
- Kubernetes Bad Practices: Automated iptables Management Disabled
- Kubernetes Bad Practices: Kernel Defaults Overridden
- Kubernetes Bad Practices: Kubelet Streaming Connection Timeout Disabled
- Kubernetes Bad Practices: Missing NodeRestriction Admission Controller
- Kubernetes Bad Practices: Missing PodSecurityPolicy Admission Controller
- Kubernetes Bad Practices: Missing Security Context
- Kubernetes Bad Practices: Missing SecurityContextDeny Admission Controller
- Kubernetes Bad Practices: Missing ServiceAccount Admission Controller
- Kubernetes Bad Practices: Service Account Token Automounted
- Kubernetes Bad Practices: Shared Service Account Credentials
- Kubernetes Misconfiguration: Insecure etcd Client Transport
- Kubernetes Misconfiguration: Insecure etcd Peer Transport
- Kubernetes Misconfiguration: Missing Kubelet Certificate Authentication
- Kubernetes Misconfiguration: Missing Service Account Token Authentication
- Kubernetes Misconfiguration: Weak SSL Certificate for Kubelet

외부 암호화 키 및 번들

암호화 키는 소스 코드와 별개의 파일에 저장할 수 있지만 버전 제어 시스템에 유지됩니다. 또한 암호화 키는 인증서 및 암호화 키와 같은 암호화 개체를 저장하는 파일인 암호화 번들에 저장할 수 있습니다. 이 릴리스에서는 이러한 파일을 다음과 같이 보고합니다. *Key Management: Hardcoded Encryption Key*.
지원되는 암호화 번들 및 키 파일은 다음과 같습니다.

- 공개 키 암호화 표준 #12 KeyStore
- Oracle의 KeyStore 형식인 Java KeyStore
- Ruby On Rails 마스터 키
- PuTTY 개인 키
- Microsoft BitLocker 암호 해독 키

기타 정정표

이번 릴리스에서는 오탐지 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.

Insecure Transport: Weak SSL Protocol

SSL(Secure Sockets Layer) 및 TLS(전송 계층 보안)는 네트워크를 통해 전송되는 데이터를 보호하는 메커니즘을 제공합니다. 이 릴리스에서는 *Insecure Transport: Weak SSL Protocol* 에 대한 지원을 업데이트했습니다. 이 릴리스부터 모든 SSL 버전 사용에 플래그를 지정하는 것 외에도 TLS 버전 1.0 또는 1.1 사용에 플래그를 지정합니다.

Insecure Transport: Weak SSL Cipher

암호 제품군은 SSL(Secure Sockets Layer) 또는 TLS(전송 계층 보안)와 함께 사용되는 암호화 알고리즘을 지정합니다. 과거에 Fortify WebInspect에서 보고한 *Insecure Transport: Weak SSL Cipher* 결과는 이제 Fortify Static Code Analyzer(SCA)에서도 보고됩니다.

Weak Cryptographic Signature

디지털 서명은 디지털 메시지의 신뢰성과 무결성을 확인하는 데 사용되는 기술입니다. DSA(디지털 서명 알고리즘)는 이제 사용되지 않으며 더 이상 사용하지 않아야 합니다. 이 릴리스에는 Java, Ruby 및 PHP에서 DSA가 사용될 때 *Weak Cryptographic Signature* 에 플래그를 지정할 수 있는 지원이 포함됩니다.

마이너 노드에 대한 지원 개선

'net', 'http', 'https' 및 'os'를 포함한 Node.js 패키지에 대한 지원을 개선했습니다. 고객은 *Cross-Site Scripting, Server-Side Request Forgery* 및 *System Information Leak* 범주에서 보다 정확한 결과를 기대할 수 있습니다.

오탐지 개선 사항:

이 릴리스에서는 오탐지를 제거하기 위한 작업과 노력이 계속되었습니다. 다른 개선 사항 외에도 다음 영역에서 오탐지가 추가로 제거될 것으로 기대할 수 있습니다.

- Credential Management: Hardcoded API Credentials(GitHub 액세스 토큰 식별 시)
- Java 애플리케이션의 Cross-Site Scripting: Content Sniffing
- "Portability Flaw: Locale Dependent Comparison"에 대한 간헐적인 오탐지
- "OGNL Expression Injection: Double Evaluation"에 대한 간헐적인 오탐지
- Password Management: Hardcoded Password(example.com과 같은 예시 도메인 내에서 설정된 경우)
- SQL Injection: iBatis Data Map

CyberRes Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase는 SmartUpdate를 통해 즉시 사용할 수 있는 다음 업데이트에서 사용자를 안내하는 정책과 수천 가지의 취약점 검사를 결합합니다.

취약점 지원 Dangerous File Inclusion: Local

Grafana는 모니터링 및 관찰을 위한 오픈 소스 플랫폼입니다. Grafana의 일부 버전은 CVE-2021-43798로 식별된 directory traversal에 취약합니다. 이 취약점은 로컬 파일에 대한 액세스를 허용합니다. 공격자가 서버에서 파일의 콘텐츠를 찾아낼 가능성도 있으며, 이는 민감한 데이터 공개 및 독점 비즈니스 로직의 잠재적인 복구로 이어질 수 있습니다. 이 릴리스에는 Grafana에서 이 취약점을 감지하기 위한 검사가 포함됩니다.

정책 업데이트 Aggressive Log4Shell[1]

지원되는 정책의 SecureBase 목록에 새로운 Aggressive Log4Shell 정책이 추가되었습니다. 기존 정책에 비해 Log4j를 사용하는 웹 애플리케이션에 대한 포괄적인 보안 평가를 위해 보다 정확하고 적극적이며 결정적인 검사를 수행할 수 있습니다. 여기에는 취약한 Apache Log4j 라이브러리 버전의 *JNDI Reference Injections*이 포함됩니다.

기타 정정표

이번 릴리스에서는 오탐지 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.

Log4Shell[1]

이 릴리스에는 Apache Log4j 라이브러리의 취약한 버전에서 *JNDI Reference Injections*에 대한 보다 정확한 검사를 제공하는 새로운 Aggressive Log4Shell 정책에 대한 지원을 추가하기 위해 Log4Shell 검사의 개선 사항이 포함됩니다.

CSRF 업데이트

이 릴리스에는 오탐지를 줄이고 결과의 정확도를 향상시키기 위한 향상된 CSRF 검사가 포함됩니다.

---

[1] *Log4Shell* 검사 및 *Aggressive Log4Shell* 정책에는 WebInspect 21.2.0.117 패치 이상이 필요합니다.

CyberRes Fortify Premium Content

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

CyberRes Fortify Taxonomy: 소프트웨어 보안 오류

새로 추가된 범주 지원에 대한 설명이 포함된 Fortify Taxonomy 사이트는 https://vulncat.fortify.com 에서 이용할 수 있습니다.마지막으로 지원되는 업데이트가 포함된 기존 사이트를 찾는 고객은 CyberRes Fortify 지원 포털에서 얻을 수 있습니다.

Fortify 기술 지원 연락처

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR 연락처

Alexander M. Hoole
선임 관리자, Software Security Research CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Software Security Research 관리자
CyberRes Fortify
peter.blay@microfocus.com

© Copyright 2022 Micro Focus or one of its affiliates. The information contained herein is subject to change without notice. The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.