Fortify Software Security Content

2024 Update 2
June 28, 2024

About OpenText Fortify Software Security Research

The Fortify Software Security Research team translates cutting-edge research into security intelligence that powers the Fortify product portfolio – including OpenText™ Fortify Static Code Analyzer and OpenText™ Fortify WebInspect. Today, Fortify Software Security Content supports 1,660 vulnerability categories across 33+ languages and spans more than one million individual APIs.

Fortify Software Security Research (SSR) is pleased to announce the immediate availability of updates to Fortify Secure Coding Rulepacks (English language, version 2024.2.0), Fortify WebInspect SecureBase (available via SmartUpdate), and Fortify Premium Content.

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

With this release, the Fortify Secure Coding Rulepacks detect 1,435 unique categories of vulnerabilities across 33+ languages and span over one million individual APIs. In summary, this release includes the following:

Improved Support for Node.js (version supported: 21.x)[1]

Node.js is a cross-platform JavaScript runtime environment that enable developers to create servers, web applications, command line tools, and more. This release contains significant updates to our Node.js support for the following modules in Node.js 21.x:

- async_hooks
- buffer
- child_process
- crypto
- dgram
- dns
- fs
- http
- https
- net
- os
- path
- process
- punycode
- querystring
- stream
- string_decoder
- timers
- tls
- url
- util
- v8
- vm
- worker_threads
- zlib

These updates improve issue detection for the following weakness categories:

- Command Injection
- Dynamic Code Evaluation: Code Injection
- Header Manipulation

[1] Requires Fortify Static Code Analyzer 24.2 or later.

- Insecure Transport: Weak SSL Cipher
- Insecure Transport: Weak SSL Protocol
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- System Information Leak: External

Additionally, the following weakness categories are introduced in this release for Node.js applications:

- DNS Spoofing
- Dynamic Code Evaluation: Script Injection
- Insecure Transport: Insufficient Diffie Hellman Strength
- Key Management: Empty HMAC Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Stream Cipher

Improved Support for Java (version supported: 21)

Java 21 is the latest long-term support (LTS) version for the Java platform. It includes enhancements to existing APIs but also includes a significant number of new features, some of the most significant ones are: Foreign Function and Memory, Sequenced Collections, Key Encapsulation, Virtual Threads, Structured Concurrency, Unnamed Variables and Scoped Values. Some of these features are still in preview state, but considered mature enough to include coverage. Updated categories include the following:

- Process Control
- Unreleased Resource
- Weak Encryption
- Weak Cryptographic Hash

Additionally, the following new categories are supported:

- Restricted Method
- Weak Cryptographic Signature: XML Signature Secure Validation Disabled

Improved MyBatis Support (version supported: 3.5.x)

MyBatis is a SQL mapper used to couple objects in a relational database with objects in an object-oriented application. This framework pairs stored procedures and SQL statements using XML descriptors or code annotations to ease the development process and database communication. Support for MyBatis has been brought up to version 3.5.16. Improvements include updated support for the following weakness categories:

- Dynamic Code Evaluation: Unsafe Deserialization
- SQL Injection
- System Information Leak
- Unreleased Resource: Database
- Unsafe Reflection

MyBatis-Plus Initial Support (version supported: 3.5.x)

MyBatis-Plus builds upon the existing MyBatis framework to simplify development by providing useful and efficient out-of-the-box features beyond those found in the original framework. Initial support for MyBatis-Plus 3.5.x is provided. Initial category support is provided for *SQL Injection*.

Detecting Risk Originating from Artificial Intelligence (AI) and Machine Learning (ML) Models

With the use of generative AI and large language models (LLMs) rapidly changing the solution space of the software industry, new risks are presenting themselves. This release improves coverage for projects that consume OpenAI APIs (Python and JavaScript), TensorFlow (Python), or Anthropic Claude (Python and JavaScript). Support detects weaknesses resulting from implicit trust of responses from AI/ML model APIs, in addition to the following features:

Improved Support for OpenAI (version supported: 1.14.x [Python], 4.33.x [JavaScript])

The OpenAI libraries for Python, TypeScript, and JavaScript provide comprehensive tools for integrating advanced AI capabilities into various applications. These libraries support a range of functionalities, including natural language processing, text generation, and conversational AI. With intuitive and user-friendly APIs, developers can seamlessly embed OpenAI's state-of-the-art AI models into their projects, enhancing interactivity and intelligence across Python, TypeScript, and JavaScript environments. Improved support expands coverage for *Cross-Site Scripting: AI*, and adds two new weakness categories:

- Cross-Site Scripting: DOM AI
- Prompt Injection

TensorFlow (version supported: 2.16.x)

TensorFlow, a leading open-source machine learning framework by Google, offers a powerful suite of tools for creating and deploying machine learning models. With built-in libraries and pre-trained models, it simplifies building deep learning applications. TensorFlow is scalable for a diverse collection of projects, ranging from research prototypes to large-scale production systems. Initial coverage includes support for the following categories:

- Path Manipulation
- Privacy Violation
- System Information Leak: Internal

Additionally, support adds the new weakness category:

- Dynamic Code Evaluation: Unsafe TensorFlow Deserialization

Anthropic Claude SDK (version supported: 0.21.3 [Python], 0.20.5 [JavaScript])

The Anthropic Claude libraries for Python and JavaScript provide comprehensive tools for integrating Claude, a sophisticated AI language model, into applications. Initial coverage includes support for *Cross-Site Scripting: AI*, and adds two new weakness categories:

- Cross-Site Scripting: DOM AI
- Prompt Injection

Improved Django Support (version supported: 5.0.x)

Django is a web framework written in Python that has been designed to facilitate secure and rapid web development. Speed and security of development are attained by the high level of abstraction in the framework, where code constructs and generation are used to drastically cut back on boilerplate code. In this release, we updated our existing Django coverage to support releases up to 5.0.x.

These updates improve issue detection for the following weakness categories:

- Access Control: Database
- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Cross-Frame Scripting
- Cross-Site Request Forgery
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Transport
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Privacy Violation: BREACH
- SQL Injection

Paramiko Initial Support (version supported: 3.4.x)

Paramiko is a Python library for connecting to machines via SSH. Paramiko provides a suite of functionalities to abstract the cryptographic methods from the developer. This provides high level functions similar to socket programming and grants developers access to the lower-level methods for

micromanagement configuration of an SSH connection. Initial support covers the following weakness categories:

- Command Injection
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Cipher
- Password Management: Hardcoded Password
- SSH Misconfiguration: Missing Authentication

Improved Support for PHP (version supported: 8.3)

PHP is a widely used general purpose scripting language that is most often used for web development. This release updates support for PHP up to version 8.3. In particular, the release includes improved support for the following extensions:

- DOM (version supported: 8.3)

  PHP's DOM extension allows for operations on XML and HTML documents in PHP by use of a document object model. Expanded support for this library includes improved dataflow support for DOM operations as well as additional coverage for identifying *Setting Manipulation* weaknesses.

- JSON (version supported: 8.3)

  PHP's JSON extension allows for use of a JSON parser written for and licensed under the PHP license. Initial support of this extension includes dataflow support for the extension's functions.

- OpenSSL (version supported: 8.3)

  PHP's OpenSSL extension implements features from the OpenSSL library for a variety of cryptographic operations. Expanded support for this library includes improved dataflow support for cryptographic key pairs.

- Simdjson (version supported: 8.3)

  PHP's Simdjson extension implements the PHP specific bindings of the simdjson project to provide fast JSON decoding. Initial support includes the following new category for PHP:

  - JSON Path Manipulation

Improved Support for iOS (version supported: 17)[2]

Apple's iOS and IPadOS SDK provides a collection of frameworks that enable developers to build mobile applications for Apple iPhone and iPad devices. This release contains incremental updates to our iOS SDK support for Swift and Objective-C. New and updated rules extend our API coverage of the following frameworks in iOS 17:

- CryptoKit

[2] iOS 17 APIs requires Xcode 15 or above, which in turn requires Fortify Static Code Analyzer 23.2 or later. However, there might be compiler warnings when using Source Code Analyzer 23.2 to build apps that use iOS 17 APIs. Fortify Static Code Analyzer 24.2 or later is recommended to ensure valid compilation and scans.

- Foundation
- Network
- os
- System
- SwiftUI
- UIKit

These updates improve issue detection for the following weakness categories:

- Insecure Transport
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- System Information Leak: External
- System Information Leak: Internal
- Unreleased Resource: Synchronization
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: User-Controlled Salt
- Weak Encryption: User-Controlled Key Size

Improved MISRA C 2012 Support

MISRA is a standards organization that creates and maintains various standards for applications development used in safety critical environments that necessitate high integrity or high reliability in software. This release includes support of two new categories that strongly map to two mandatory guideline rules in the MISRA C 2012 standard:

- Undefined Behavior: File Pointer Dereference
- Undefined Behavior: File Pointer Use After Close

Password Regular Expression Properties Update

The password regular expression properties, introduced in Fortify Static Code Analyzer version 23.1, are customizable properties containing regular expressions that dictate how Fortify rules match password identifiers in various languages. In this release, we expanded the default value of the com.fortify.sca.rules.password_regex.global property to recognize password identifiers involving the word "secret". Additionally, we added new rules to utilize the password regular expression properties in analyzing dynamically generated JSON strings. As a result, customers can expect improved detection in the following categories across languages:

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Privacy Violation

Improved Support for Golang (version supported: up to 1.21)
Go, also known as Golang, is a compiled, statically typed programming language created at Google. It's known for its simplicity, efficiency, and strong support for concurrency, making it ideal for building

scalable web services, data pipelines, and distributed systems. This release includes detection for *Unreleased Resource* weaknesses and introduces new *SQL Injection* detection for projects using GORM v2.

WordPress API Improvements (version supported: up to 6.5) (API count: 2)

The WordPress Application Programming Interface (API) can be separated into multiple API sections / topics, each covering the functions involved in, and use of, a given set of functionalities. Together they form what might be called the WordPress API, which is the plugin/theme/add-on interface created by the entire WordPress project. This release adds initial support for identifying issues in the following APIs:

- REST API
- Shortcode API

Miscellaneous Errata

In this release, resources have been invested to ensure we can reduce the number of false positive issues, refactor for consistency, and improve the ability for customers to audit issues. Customers can also expect to see changes in reported issues related to the following:

False Positive Reduction and Other Notable Detection Improvements

Work has continued with the effort to remove false positives in this release. Customers can expect further removal of false positives, and other notable improvements related to the following areas:

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* – false positives reduced in ASP.NET applications
- *Insecure Transport: Mail Transmission* – false positives reduced in Java applications
- *Password Management: Hardcoded Password* – false positives reduced in JSON/YAML files
- *Unreleased Resource: Streams* – false positives reduced in Java applications
- *Password Management: Hardcoded Password* – new issues detected in Python applications related to dictionary types
- *Password Management: Hardcoded Password* – new issues detected in ASP.NET applications related to interpolated strings
- Many false positives removed coming from built-in JDK system properties

Category Name Changes

When weakness category name changes occur, merging analysis results of prior scans with new scans might result in added/removed categories.

To improve consistency, the following three categories have been renamed:

2024 R1 Category Name	2024 R2 Category Name
Access Control: gRPC Authentication Bypass	Access Control: gRPC Fail Open

AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS CloudFormation Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key
AWS Terraform Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key

DISA Control Correlation Identifier (CCI) Version 2

Defense Information Systems Agency (DISA) CCI is a document that bridges the gap between high- and low-level cybersecurity guidance by providing a set of standard identifiers paired with singular, actionable statements. The DISA Application Security and Development STIG is closely mapped to DISA CCI wherein a single STIG control may apply to one or more CCI. This release brings mapped CCIs to parity with the recent updates to STIG mappings against the Fortify taxonomy during the prior releases.

NIST Special Publication 800-53 Revisions 4 and 5

The National Institute of Standards and Technology (NIST) Special Publication 800-53 is a document that provides a catalog of security and privacy controls for information systems that may be leveraged by the cybersecurity field at large to provide guidance on how to secure systems. NIST Special Publication 800-53 is closely mapped to the DISA CCI, wherein a single CCI may apply to one or more NIST 800-53 control. This release brings mapped NIST 800-53 controls to parity with the recent updates to DISA CCI mappings against the Fortify taxonomy.

OWASP Mobile Top 10 2023

As previously announced, in this release of Fortify Software Security Content, the OWASP Mobile Top 10 2023 mapping is now deprecated and only the updated OWASP Mobile Top 10 2024 remains.

Aligning Software Security Content Releases with OpenText Versioning

The next release will contain a change in the security content versioning. This will be the last OpenText Fortify Security Content Update release that follows the naming convention of "2024 Update 2". To align with OpenText versioning standards, releases are scheduled one per quarter every year, and are numbered according to the year and quarter — therefore, the next release of OpenText™ Fortify™ Software Security Content release will be 24.4, indicating a release in the first month of the 4th quarter of 2024.

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase combines checks for thousands of vulnerabilities with policies that guide customers in the following updates available immediately using SmartUpdate.

Vulnerability Support

Denial of Service: GraphQL

The GraphQL query language for APIs provides a runtime to query existing data. GraphQL schema is a model consisting of data objects, their fields and types, and their relationships to other data objects. References between different data objects can create a cycle. An attacker can trigger excessive CPU and memory usage by crafting a malicious nested and expensive cyclical query to cause a Denial of Service (DoS). This release includes a check to detect circular references in GraphQL schema.

Access Control: Authorization Bypass (CVE-2024-27198)

CVE-2024-27198 has been identified as a critical vulnerability in JetBrains software and represents a significant security threat. This vulnerability highlights the risks associated with insufficient authentication mechanisms, which can allow unauthenticated attackers to gain administrative control over the affected systems. The latest release includes a check to detect this vulnerability on target servers.

Directory Traversal (CVE-2024-27199)

JetBrains TeamCity On-Premises server versions prior to 2023.11.4 are vulnerable to a path traversal flaw, identified as CVE-2024-27199. Attackers can use this flaw to bypass authentication controls, and significantly threaten system integrity and confidentiality. The latest release includes a check to detect this vulnerability on target servers.

Dynamic Code Evaluation: Unsafe Deserialization (CVE-2023-26360)

Adobe ColdFusion versions 2018 Update 15 and earlier, as well as 2021 Update 5 and earlier, are affected by a Dynamic Code Evaluation vulnerability, identified by CVE-2023-26360. This vulnerability could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. This release includes a check to detect this vulnerability on target servers.

Insecure Deployment: Unpatched Application (CVE-2024-32962)

CVE-2024-32962 is a critical vulnerability associated with xml-crypto, an XML digital signature and encryption library for Node.js. This vulnerability was introduced in version 4.0.0 and has been addressed in version 6.0.0. The vulnerability arises because, in affected versions, the default configuration does not check the authorization of the signer. An attacker can exploit this by modifying an XML document and replacing the existing signature with one generated with a malicious private key, attaching the corresponding certificate to the <KeyInfo /> element. This release includes a check to detect this vulnerability on target servers that use affected xml-crypto versions.

Miscellaneous Errata

In this release, we invested resources to further reduce the number of false positives and improve the ability for customers to audit issues. Customers can also expect to see changes in reported findings related to the following areas.

Insecure Deployment: OpenSSL

This release includes improvements for the OpenSSL ChangeCipherSpec Man-in-the-Middle (MitM) check to reduce false positives and improve the accuracy of the results.

Fortify Premium Content

The research team builds, extends, and maintains a variety of resources outside our core security intelligence products.

Fortify Taxonomy: Software Security Errors

The Fortify Taxonomy site, which contains descriptions for newly added category support, is available at https://vulncat.fortify.com.

Contact Customer Support

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

Contact SSR

Alexander M. Hoole
Senior Manager, Software Security Research
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Manager, Software Security Research
OpenText Fortify
pblay@opentext.com
+1 (669) 309-1634