Fortify Software Security Content

2024 Update 1
March 29, 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 (SCA) and OpenText™ Fortify WebInspect. Today, Fortify Software Security Content supports 1,654 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 2024.1.0), 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 1,429 unique categories of vulnerabilities across 33+ languages and span over one million individual APIs. In summary, this release includes the following:

Improved Support for Angular (version supported: 16.0.0)

Angular is a typescript-based, free and open source web application development framework that specializes in creating SPAs (Single Page Applications) and is mostly used at the frontend to dynamically and efficiently manipulate data. Support was expanded for Angular from version 11.2.4 through Angular 16.0.0 (initial support only). Angular results have been enhanced so that customers can expect better results around categories such as *Cross-Site Request Forgery*, *Privacy Violation,* and *System Information Leak*. Coverage was expanded for JavaScript DOM Document as well as the following modules:

- @angular/common/http
- @angular/core
- @angular/platform-browser

Improved Support for PHP (version supported: 8.2)

PHP is a widely used general purpose scripting language that is most often used for web development. The latest SSR release updates support for PHP up to version 8.2. In particular, the release includes initial support for the following additional PHP base extensions:

- Sodium (version supported: 8.3.1)

  The PHP Sodium extension is an implementation of the Libsodium library. Sodium provides capabilities for encryption, decryption, signatures, password hashing, and other cryptographic operations. Customers might find additional issues related to encryption and digital signatures, along with changes around Privacy Violation issues.

- Zip (version supported: 1.22.3)

  The PHP Zip extension is an implementation of the Libzip library. Zip provides capability for creation, modification, and reading of zip archives, a common structure used to accomplish file/data grouping and compression. Initial support of the extension includes coverage of the ZipArchive class specific to basic filesystem dataflow and expansion of PHP coverage for the following categories:

  - Key Management: Empty PBE Password
  - Path Manipulation: Zip Entry Overwrite

Improved Support for Golang (version supported: 1.21)[1]

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. Go combines the performance benefits of compiled languages with the ease of programming seen in interpreted languages. Its concise syntax and powerful standard library enable developers to write robust code quickly. Coverage is expanded for the following packages:

- context
- crypto/ecdh
- html/template
- net
- reflect
- Runtime
- time

Cloud Infrastructure as Code (IaC)[2]

Expanded support for cloud infrastructure as code. Infrastructure as code is the process of managing and provisioning computer resources through code, rather than various manual processes. Common issues related to the configuration of these services mentioned are now reported to the developer. As of Fortify Static Code Analyzer 24.2 Azure ARM and AWS CloudFormation configuration issues are reported using new techniques. This results in a set of added and removed issues when merging FPRs generated with prior versions of Fortify Static Code Analyzer. With Fortify Static Code Analyzer 24.2 and later, the 2024.1 Rulepacks are required to prevent duplicate IaC issues.

Azure Resource Manager (ARM) Configurations

ARM is the deployment and management service for Azure. ARM provides a management layer that enables you to create, update, and delete resources in your Azure account.

Amazon Web Services (AWS) CloudFormation Configurations

CloudFormation is a service provided by Amazon that is used to automate the provisioning and configuration of AWS resources. CloudFormation enables users to manage AWS resources using a JSON or YAML template. Utilizing these templates, users can create, delete, and modify collections of resources, known as a stack, as a single unit. In this release, we report the following additional weakness categories for AWS CloudFormation configurations:

- AWS CloudFormation Misconfiguration: Insecure SageMaker Transport
- AWS CloudFormation Misconfiguration: SageMaker Network Isolation Disabled
- AWS CloudFormation Misconfiguration: Weak SecretsManager Generated Password

[1] For optimal results, upgrade to Fortify Static Code Analyzer 24.2 or later.
[2] Requires Fortify Static Code Analyzer 24.2 or later.

Improved Kotlin Support (version supported: 1.9.2)[3]

Kotlin is a general-purpose, statically-typed language featuring Java interoperability. This release includes updated support for new standard library APIs introduced in Kotlin 1.7.2, 1.8, and 1.9 targeting Kotlin namespaces: *jvm.optional*, *math*, *io.path*, *coroutines.cancellation,* and *kotlinx.serialization.json*. Additional issues might be detected in existing categories, including:

- Denial of Service: Regular Expression
- Path Manipulation
- Privacy Violation
- System Information Leak

JavaScript/TypeScript Node.js Improvements[4]

Our Node.js rules have been updated to benefit from type resolution when using Fortify Static Code Analyzer 24.2. The changes result in reduced false positives, improved true positives, and more accurate findings in Node.js applications across most categories. More specifically, customers can expect improved results related to the following Node.js modules:

- child_process
- dgram
- dns
- fs
- http
- https
- net
- querystring
- tls
- url
- util
- v8

Initial partial support for the following NPM packages is also included:

- Bluebird
- child-process-promise

Improved DISA STIG 5.3 Support

To support our federal customers in the area of compliance, correlation of the Fortify Taxonomy to the Defense Information Systems Agency (DISA) Application Security and Development STIG version 5.3 has been updated to include the following 45 additional STIG IDs: APSC-DV-000010, APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000330, APSC-DV-000380, APSC-DV-000390, APSC-DV-000400, APSC-DV-000410, APSC-DV-000430, APSC-DV-000450, APSC-DV-000580, APSC-DV-000590, APSC-DV-000710, APSC-DV-001120, APSC-DV-001130, APSC-DV-001280, APSC-DV-001290, APSC-DV-001300, APSC-DV-001310, APSC-DV-001320, APSC-DV-001330, APSC-DV-

[3] Kotlin 1.9 support requires Fortify Static Code Analyzer 24.2 or later.

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

001410, APSC-DV-001520, APSC-DV-001530, APSC-DV-001540, APSC-DV-001610, APSC-DV-001760, APSC-DV-001770, APSC-DV-001780, APSC-DV-001790, APSC-DV-001795, APSC-DV-001820, APSC-DV-001970, APSC-DV-002290, APSC-DV-002310, APSC-DV-002320, APSC-DV-002410, APSC-DV-002530, APSC-DV-002890, APSC-DV-002950, APSC-DV-002960, APSC-DV-003100, APSC-DV-003310, and APSC-DV-003320.

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:

- *Access Control: Anonymous LDAP Bind* – false positives removed in C/C++ applications
- *Command Injection* – new issues detected in C/C++ applications that use Windows variant of C runtime library functions
- *Credential Management: Hardcoded API Credentials* – false positives removed in YAML files
- *Dockerfile Misconfiguration: Dependency Confusion* – false positives removed in Dockerfiles involving npm
- *Dynamic Code Evaluation: Code Injection* – new issues detected in ASP.NET applications that use Azure Cosmos DB APIs
- *GCP Terraform Misconfiguration: Insecure Supply Chain* – false positives removed in AWS Terraform configuration files
- *Insecure SSL: Server Identity Verification Disabled* – new issues detected in Python applications that use the `Requests` library
- *Mass Assignment: Insecure Binder Configuration* – false positives removed in ASP.NET MVC applications
- *Mass Assignment: Request Parameters Bound into Persisted Objects* – false positives removed from Spring applications
- *Password Management: Hardcoded Password* – new issues detected in ODBC connection strings
- *Poor Style: Identifier Contains Dollar Symbol ($)* – false positives removed in Java applications
- *Privacy Violation* – new issues detected in ASP.NET applications that use Razor Pages
- *Privacy Violation* – new issues detected in Dart/Flutter applications
- *Privacy Violation* – new issues detected in JavaScript applications that use the `csurf` middleware along with ExpressJS library
- *String Termination Error* – new issues detected in C/C++ applications
- *System Information Leak: External* – new issues detected in ASP.NET applications that use Razor Pages
- *System Information Leak: External* – new issues detected in C/C++ applications
- *Weak Encryption: Inadequate RSA Padding* – false positives removed in PHP applications that use OpenSSL
- Various dataflow false positives removed in Python Django applications

- Various new dataflow issues detected in Java Spring applications
- Various dataflow issues appearing from the main() entry point in Java scans might show as new and removed. This also removes duplicates and incorrect traces found in Kotlin and Scala applications.

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 four categories have been renamed:

2023 R4 Category Name	2024 R1 Category Name
Insecure Cross-Origin Opener Policy	HTML5: Insecure Cross-Origin Opener Policy
Insecure Transport: Client Identity Verification Disabled	Insecure SSL: Server Identity Verification Disabled
Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control	Kubernetes Terraform Misconfiguration: Improper DaemonSet Access Control
Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control	Kubernetes Terraform Misconfiguration: Improper StatefulSet Access Control

Deprecation of the "Header Checking Disabled" category

The category has been removed to avoid confusion with other similarly named categories. Previous rules in this category now report in:

- ASP.NET Misconfiguration: Header Checking Disabled
- ASP.NET Misconfiguration: Unsafe Header Parsing

Deprecation of certain "Dead Code" categories

The following "Dead Code" categories have been removed from the standard Rulepacks:

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: Unused Field
- Dead Code: Unused Method
- Dead Code: Unused Parameter

For customers that want to continue seeing these vulnerabilities detected, the rules can be downloaded from Fortify Support Portal in a separate Rulepack.

Renaming and Deprecation of OWASP Mobile Top 10 2023

Following the release of the “OWASP Top 10 Mobile Risks – Initial Release 2023” in September 2023, the project was finalized and renamed “OWASP Top 10 Mobile Risks – Final Release

2024” in January 2024. As a result, this release includes an additional and renamed mapping for “OWASP Mobile Top 10 Risks 2024”. The mappings themselves have no functional changes.

In the next release of Fortify Software Security Content, the OWASP Mobile Top 10 2023 mapping will be deprecated and only the updated OWASP Mobile Top 10 2024 will remain.

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

Insecure Deployment: Unpatched Application (CVE-2024-23897)

Jenkins is a Java-based automation server that is used to build, test, and deploy software. Jenkins Command Line Interface (CLI) is a built-in feature of Jenkins that provides a way to interact with the Jenkins server and is enabled by default. A critical file read vulnerability identified by CVE-2024-23897 allows for arbitrary file read capabilities in Jenkins. This vulnerability is present in the args4j library that is used to parse command arguments and options supplied to the CLI. The command parser has a feature that replaces the at sign (@) character followed by a file path in an argument with the contents of the specified file. The affected versions of Jenkins include 2.441 and earlier and LTS 2.426.2 and earlier. This release includes a check to detect CVE-2024-23897 on a target server.

Insecure Deployment: Unpatched Application (CVE-2023-22515)

Atlassian Confluence Data Center and Confluence Server are self-managed solutions known for providing organizations with best practices for collaboration. A critical broken access control vulnerability identified by CVE-2023-22515 allows malicious actors to create unauthorized administrator accounts, granting them unrestricted access to the Confluence platform. Even when attackers lack authentication, they can take advantage of CVE-2023-22515 to establish unauthorized administrator accounts and gain access to Confluence instances. Attackers can also manipulate the Confluence servers settings to suggest that the setup process has not been finalized. The affected versions of Confluence Server and Confluence Data Center are 8.0.0-8.0.4, 8.1.0-8.1.4, 8.2.0-8.2.3, 8.3.0-8.3.2, 8.4.0-8.4.2, and 8.5.0-8.5.1. This release includes a check to detect CVE-2023-22515 on a target server.

Insecure Deployment: Unpatched Application (CVE-2023-22518)

A critical improper authorization vulnerability identified by CVE-2023-22518 affects Atlassian Confluence Data Center and Confluence Server. This vulnerability allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can perform all administrative actions that are available to a Confluence instance administrator causing a full loss of confidentiality, integrity, and availability. The affected

versions of Confluence Server and Confluence Data Center are all versions prior to 7.19.16 and versions 8.3.4, 8.4.4, 8.5.3, and 8.6.1. This release includes a check to detect CVE-2023-22518 on a target server.

OGNL Expression Injection: Double Evaluation (CVE-2023-22527)

A critical OGNL Expression Injection vulnerability identified by CVE-2023-22527 affects Atlassian Confluence Server and Data Center. This vulnerability allows an unauthenticated attacker to execute arbitrary code on vulnerable applications. The affected versions of Confluence Data Center and Confluence Server are 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0-8.5.3. This release includes a check to detect this vulnerability in affected Atlassian servers.

Compliance Reports

Improved DISA STIG 5.3

To support our federal customers in the area of compliance, correlation of the Fortify Taxonomy to the Defense Information Systems Agency (DISA) Application Security and Development STIG version 5.3 has been updated to include the following 8 additional STIG IDs: APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000450, APSC-DV-001280, APSC-DV-001300, APSC-DV-002530, and APSC-DV-003320.

Policy Updates

Improved DISA STIG 5.3

DISA STIG 5.3 policy is updated to include additional checks relevant to DISA STIG 5.3.

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.

XPath Injection

This release includes improvements for the *XPath Injection* 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.

OWASP Mobile Top 10 2024

To accompany the renamed OWASP Mobile Top 10 Risks 2024 correlations, this release also contains a new report bundle for OpenText™ Fortify Software Security Center with support for OWASP Mobile Top 10 2024, which is available for download from the Fortify Customer Support Portal under Premium Content.

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 Fortify 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