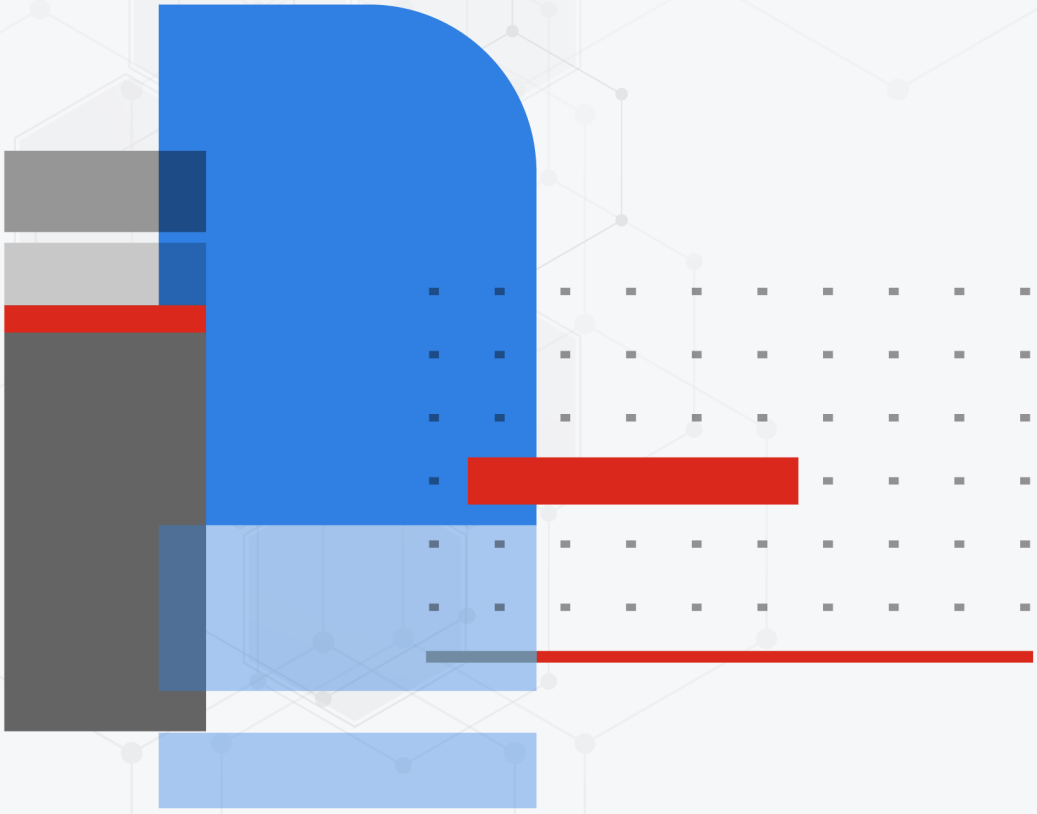
Release Notes

FortiDevSec 24.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 18, 2024
FortiDevSec 24.4.0 Release Notes
68-244-1108129-20241218

TABLE OF CONTENTS

Change Log

Date	Change description
2024-12-18	FortiDevSec version 24.4.0 release document.

Introduction

FortiDevSec is a cloud-based automated application security tool that performs intensive and comprehensive scans for an accurate vulnerability assessment of your application. It integrates continuous application security testing into major DevOps Continuous Integration (CI) Continuous Deployment (CD) environments, embedding itself into the process of developing and deploying applications to evaluate and detect security gaps that you can mitigate/remediate in the course of the Software Development LifeCycle (SDLC). The automated scanning process resides in your CI/CD pipeline and allows you to scan your applications without manual intervention and is completely non-intrusive with no disruptions to your setup. The easy-to-understand application security assessment approach of FortiDevSec allows you to build secure applications and involves a simple 3-step procedure that facilitates application scanning with minimal know-how of the application security domain. For detailed product overview, configuration, and usage procedures see the *FortiDevSec User Guide*.

What's New

This release of FortiDevSec includes performance optimizations and bug fixes.

Note: Scanner docker images must be updated using `docker pull <image>` command to the latest version to use the new features.

Product Integration and Support

The following table lists the latest supported/tested web browsers for FortiDevSec version 24.4.0:

Item	Supported version
Web browser	• Microsoft Edge version 122.0.2365.92 (Official build) (64-bit) • Mozilla Firefox version 124.0 (64-bit) • Google Chrome version 122.0.6261.129 (Official Build) (64-bit) • Apple Safari version 17.4 Other web browsers may work correctly but Fortinet does not support them.

Resolved Issues

The following issues have been resolved inFortiDevSec version 24.4.0.

Issue ID	Description
1095898	Both success and warning messages are displayed when attempting to configure the Jira plugin, FortiDAST plugin and risk rating page with read-only access permissions.
1099730	Users of member groups are not notified of name, visibility, or application changes in associated application groups.
1094878	A warning message is not displayed when adding an application to an application group that is already a member of another application group.

Known Issues

The following are known issues in FortiDevSec version 24.4.0.

Issue ID	Description
1083257	The *Vulnerability Catalog* page may experience slow loading times when displaying vulnerabilities.
1083256	The *file path*, *outbreak alert links*, and *similar occurrence data* are missing in the report exported from *Vulnerability Catalog* page.
1076581	The *consolidated scan results API* may generate incomplete data in the *result.csv* file when the *group instances* field exceeds 32,760 characters.
1012904	JFrog CI integration with GitHub/GitLab is not populating Branch ID and Commit ID.
891704	Scans initiated from the master user account on sub user's account fails if the sub user has not logged in to FortiDevSec GUI at least once.
1049531	Inconsistent vulnerability count in *Analytics >Organization Level >Top Vulnerable Apps* section for demo accounts.
1093537	Users with read permission are able to perform SAST and DAST scans.
1099238	*Accept* and *Reject* links in the notification email for shared group join request are not redirecting to the *Group Requests* page.
1083255	*Vulnerabilities* widget in *App Directory > Application* page displays incorrect vulnerability counts by severity.
1050034	Vulnerability Compliance chart missing in organization level PDF report for some users.

www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.