

Release Notes

FortiDevSec 23.1



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

January 23, 2023

FortiDevSec 23.1 Release Notes

TABLE OF CONTENTS

Change log	4
Introduction	5
What's New	6
Product integration and support	7
Known issues	8

Change log

Date	Change description
2023-01-23	FortiDevSec version 23.1 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 the following new features.

Feature	Description
Outbreak Alerts	The FortiDevSec now displays FortiGuard outbreak alerts identified after performing the application scan. FortiDevSec users can navigate to FortiGuard Outbreak Alert page for in-depth analysis of the vulnerability. This feature is currently available for SCA and Container scanners.
CVE details	The CVE details for the SCA and Container scanners are now displayed in the vulnerability details page.
Default DAST scanner	The default DAST scanner FortiPenTest is renamed as FortiDAST.
Remediation	The FortiDevSec scan results now include Remediation field in the identified vulnerability details page that provides information (if available) on how to fix/avoid the vulnerability. This feature is supported for SCA, Container, and FortiDAST scanners.

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 23.1:

Item	Supported version
Web browser	<ul style="list-style-type: none">• Microsoft Edge version 105.0.1343.42• Mozilla Firefox version 104.0.2• Google Chrome version 105.0.5195.127• Apple Safari version 15.3 <p>Other web browsers may work correctly but Fortinet does not support them.</p>

Known issues

The following issues are known in FortiDevSec version 23.1.

Issue ID	Description
861630	The FortiDAST asset scan configuration details can only be added by logging in to FortiDAST after performing the initial scan.
876413	[FortiDAST Proxy] Scan fails when FQDN of the internal asset is used as target.

