

Release Notes

FortiDAST 23.2.0



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

May 20, 2023

FortiDAST 23.2.0 Release Notes

67-232-913911-20230520

TABLE OF CONTENTS

Change log	4
Introduction	5
Product integration and support	7
What's new	8
Resolved issues	9
Known issues	10

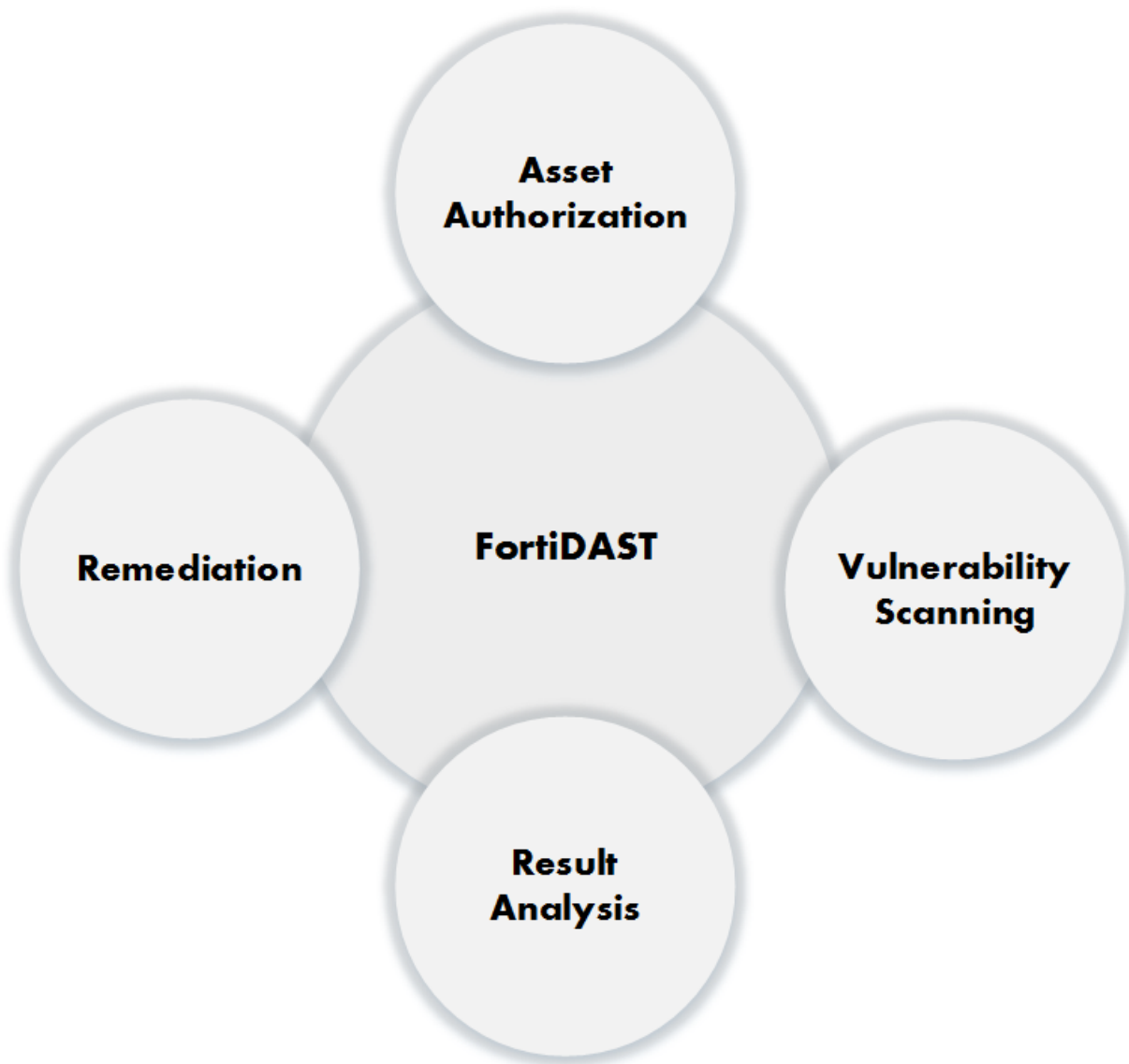
Change log

Date	Change description
2023-05-20	FortiDAST version 23.2.0 release document.

Introduction

FortiDAST is a cloud enabled service that performs vulnerability assessment and penetration testing through an intensive process of comprehensive and criteria based automated scanning and analysis. It adopts an organised technical approach of assessing your web applications running in an HTTP/HTTPS environment, to identify loopholes and vulnerabilities. Penetration testing (pen-testing) is the process to explore and exploit security vulnerabilities in an application using various malicious techniques to discover security gaps; securing your network and assisting in suitable remediation steps for the identified susceptibilities.

The goal of FortiDAST is to provide an easy-to-understand and non-intrusive evaluation of the security posture of your web applications. The outcome is an accurate and detailed vulnerability assessment report with a high vulnerability detection rate that facilitates appropriate measures for remediation and further network penetration testing.



This diagram lays down the building blocks of the FortiDAST vulnerability assessment and penetration testing service.

This document provides a list of new features and product integration information for FortiDAST version 23.2.0. Review all sections of this document before you use this service.

Product integration and support

The following table lists the latest supported/tested web browsers for FortiDAST version 23.2.0:

Item	Supported version
Web browser	• Microsoft Edge version 113.0.1774.42 (Official build) (64-bit) • Mozilla Firefox version 113.0.1 (64-bit) • Google Chrome version 113.0.5672.93 (Official Build) (64-bit) Other web browsers may work correctly but Fortinet does not support them.

What's new

The following table lists new features in FortiDAST version 23.2.0.

Feature	Description
Exploit Engine	The following exploit engine enhancements are added: • A new and improved GUI option to select and configure specific components within the exploit engine. • Detection of additional CVEs is supported.
Fuzzer enhancement	The following new Fuzzer modules are added. • Clickjacking • Malware detection

Resolved issues

The following issues have been resolved in FortiDAST version 23.2.0. For inquiries about a particular issue, visit the [Fortinet Support](#) website.

Issue ID	Description
865943	FortiDevSec DAST scan freezes when SSH is disabled between the scanner VM and the Proxy agent.
859105	SSRF vulnerabilities are not detected in the FortiDAST proxy mode.
876744	HTTP request smuggling vulnerability is not detected.
874824	Blind XXE and Blind RCE vulnerabilities are not detected.
876413	[FortiDAST Proxy] Scan fails when FQDN of the internal asset is used as target.
913904	The Code injection module reports multiple instances of false positives.
902354	Not able to configure the login URL for webauth when the targets have more than three sub-domains and a longer domain extension.

Known issues

The following issues are known in FortiDAST version 23.2.0. For inquiries about a particular issue, visit the [Fortinet Support](#) website.

Issue ID	Description
646320	Password protected reports do not have working links.
693579	The FortiWeb compatible reports contain Sensitive Data Exposure errors for queries blocked by FortiWeb.
820470	Modules that need to return the WAF Headers are not returning HTTP request headers.
820908	Partial URI rescan stops abruptly.
819333	Scans scheduled monthly are not working.
874324	[FortiDAST Proxy] C2 server is not working for FSE scripts.
876384	Failure in detecting Atlassian Jira and Confluence outbreak when using proxy in the Google Cloud Platform (GCP) configuration.
913594	The GitLab FSE CVE-2021-22205 vulnerability is not reported when using proxy. The scan freezes.
896907	False positive result for CSRF vulnerability.

www.fortinet.com



Copyright© 2023 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.