Release Notes

FortiDAST 23.3.0

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

July 06, 2023
FortiDAST 23.3.0 Release Notes
67-233-927264-20230706

TABLE OF CONTENTS

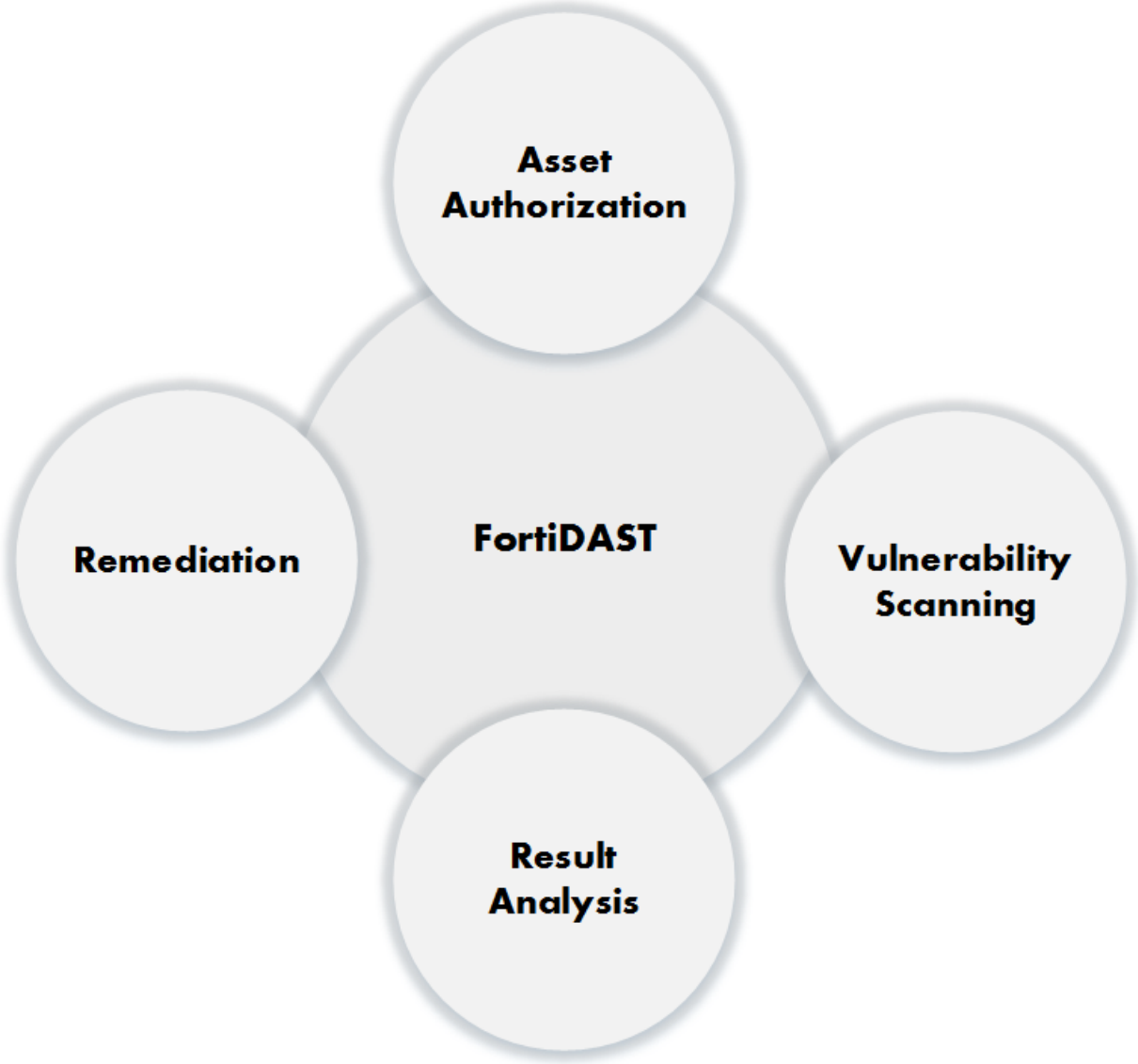
Change log

Date	Change description
2023-07-06	FortiDAST version 23.3.0 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 23.3.0. 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 23.3.0:

Item	Supported version
Web browser	• Microsoft Edge version 114.0.1823.58 (Official build) (64-bit) • Mozilla Firefox version 114.0.2 (64-bit) • Google Chrome version 114.0.5735.199 (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 23.3.0.

Feature	Description
FortiDAST integration with FortiWeb Cloud on AWS	You can now perform FortiDAST scans within FortiWeb Cloud subscribed through AWS Marketplace.
GUI enhancement	The following GUI enhancements are added: • A new scan *Progress Summary* window is added in *Scans Policy* page to view detailed information of scans in progress. • Redesigned *Scan Status* widget in *Scans Overview*> *Summary* page.
Fuzzer enhancement	*POST* method support is added for *SQL injection* and *XSS*.

Resolved issues

The following issues have been resolved in FortiDAST version 23.3.0. For inquiries about a particular issue, visit the Fortinet Support website.

Issue ID	Description
920326	Scan fails to initialize once the API definition file is added.
830478	Vulnerable API endpoint is not detected by XSS fuzzer module.
923759	Skipped URLs must be shown separately.

Known issues

The following issues are known is FortiDAST version 23.3.0. 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