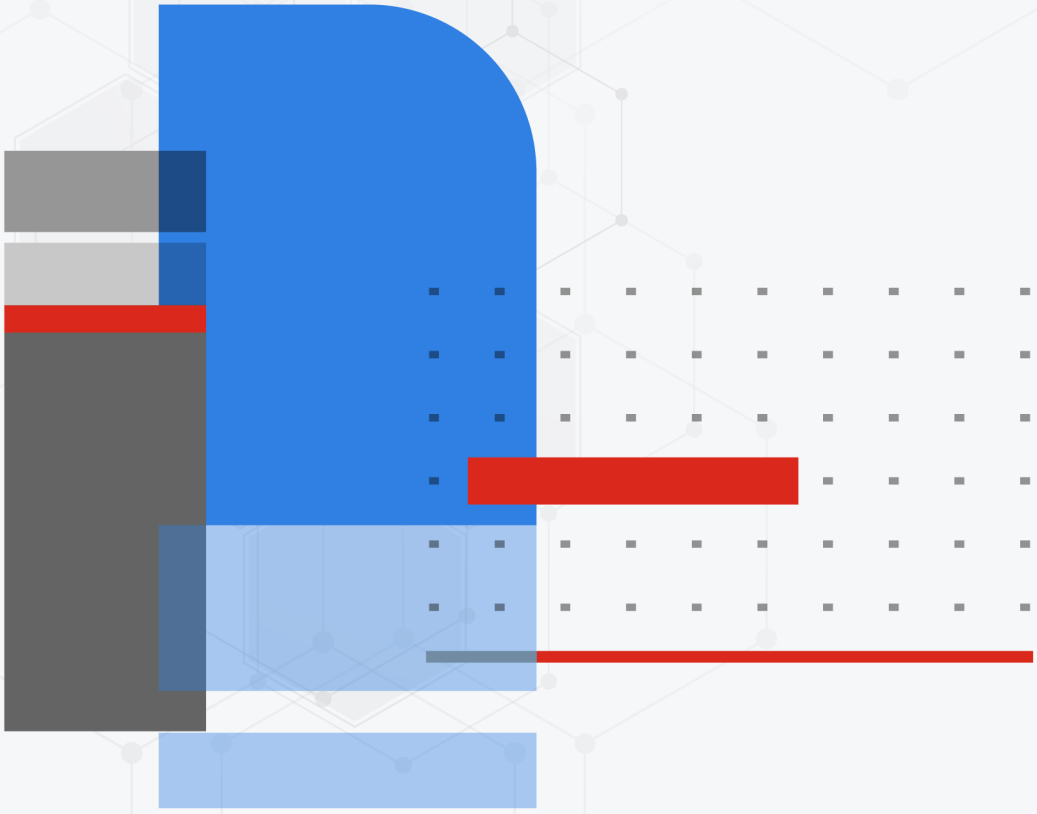
# Release Notes

**FortiDAST 24.1.0**



**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

March 28, 2024
FortiDAST 24.1.0 Release Notes
67-241-1014425-20240328

# TABLE OF CONTENTS

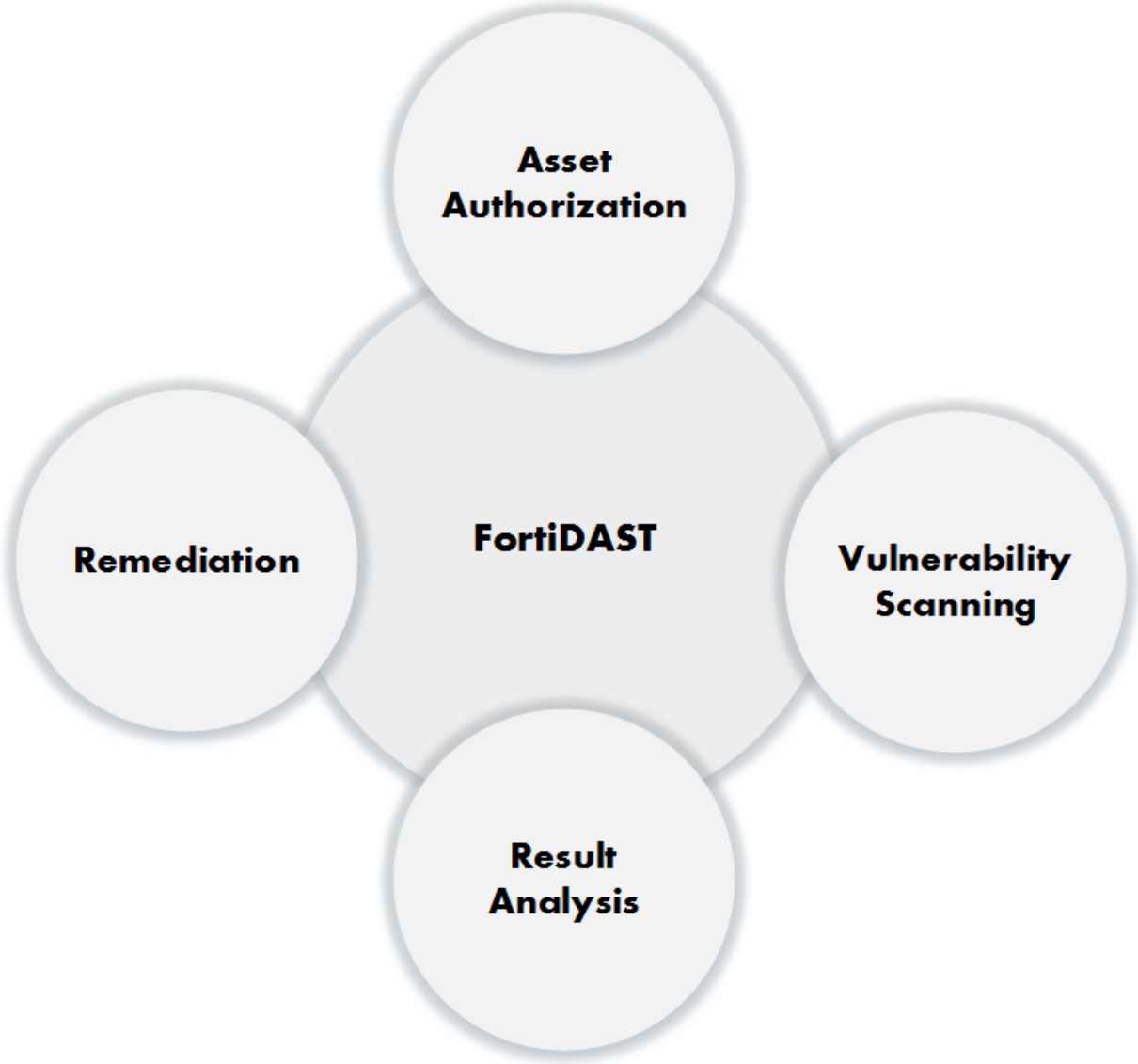
# Change log

| Date | Change description |
| --- | --- |
| 2024-03-28 | FortiDAST version 24.1.0 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 24.1.0. 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 24.1.0:

| Item | Supported version |
|---|---|
| Web browser | • Microsoft Edge version 122.0.2365.92 (Official build) (64-bit)<br>• Mozilla Firefox version 124.0.1 (64-bit)<br>• Google Chrome version 123.0.6312.58 (Official Build) (64-bit)<br>Other web browsers may work correctly but Fortinet does not support them. |

# What's new

The following table lists new features in FortiDAST version 24.1.0.

| Feature | Description |
|---|---|
| API Discovery and Crawling | If no API definition file is provided, FortiDAST automatically searches common locations and Fetch/XHR data to discover API definitions and then crawls the discovered endpoints. |
| WordPress Version Detection | FortiDAST now detects WordPress versions and identifies known vulnerabilities associated with them. The identified vulnerabilities are reported in *OWASP Category > Vulnerable and Outdated Components*. |
| Exploit Engine | Detection of additional CVEs is supported. |

# Resolved issues

The following issues have been resolved in FortiDAST version 24.1.0. For inquiries about a particular issue, visit the Fortinet Support website.

| Issue ID | Description |
|---|---|
| 1007014 | Webfilter functionality is not working as expected. |

# Known issues

The following issues are known is FortiDAST version 24.1.0. 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