FortiSIEM - Release Notes

Version 5.4.0

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

12/16/2021
FortiSIEM 5.4.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
12/16/2021	Add Known Issues - Remediation Steps for CVE-2021-44228 to 5.2.6-5.4.0 Release Notes.

Introduction

FortiSIEM provides an all-in-one, seamlessly integrated and service-oriented IT infrastructure monitoring solution that covers performance, availability, change, and security monitoring aspects of network devices, servers, and applications.

This document provides a list of resolved issues in FortiSIEM 5.4.0 Release.

What's New in 5.4.0

This release contains the following bug fixes, enhancements, new device support, and Known Issues.

- Bug Fixes and Enhancements
- New Device Support
- Known Issues

Bug Fixes and Enhancements

Bug ID	Severity	Module	Description
664708	Major	App Server	All Super Global users can see all Incidents for all Organizations, regardless of their role restrictions.
655557	Major	Query	Real time Query results not shown if there is no overlap between Event workers and Query workers.
665994	Minor	App Server	Selecting a incident category first in search panel will cause aggregation count of other criteria to be blank.
665387	Minor	App Server	Analytics filter operator IN / NOT IN doesn't work for individual CMDB selections.
664245	Minor	App Server	Incident comments filled with debug messages when running CVE Integration.
659678	Minor	App Server	Geo Maps do not show location on Dashboard map widget.
653426	Minor	App Server	Dashboard using Google API does not work for Org if the Org user does not have read permission of Google key (in Admin).
651528	Minor	App Server	FortiSIEM CMDB to ServiceNow Duplicates.
660734	Minor	Device Support	Aruba Parser parses causes high CPU because of excessive use of regular expression.
659163	Minor	Device Support	Fortigate on AWS logs are not recognized in FortiSIEM because of new devices.
652184	Minor	Device Support	Update Unix Parser with a new time stamp format.
652182	Minor	Device Support	Update F5BigIP Parser Update for Unsupported (New/Custom) Syslog Header.
649906	Minor	Device Support	CentOS CROND events incorrectly parsed as McAfee-WebGw-Run-Cmd because logs are too similar.
647216	Minor	Device Support	Not all attributes for Windows Security Events 4754, 4759, 4749 are parsed.

Bug ID	Severity	Module	Description
640196	Minor	Device Support	Not all attributes for Windows Security Event Parsing for Event ID 4625 is incorrect.
634374	Minor	Device Support	Windows Security Event ID 4688 is not parsed fully.
634372	Minor	Device Support	Windows Sysmon Parser needs to be extended.
607339	Minor	Device Support	Sysmon PowerShell Commands not correctly parsed if .exe is called from within Powershell.
594078	Minor	Device Support	Rule "Windows Audit Log Cleared" does not include user as an incident attribute.
592946	Minor	Device Support	Set Windows Event ID, Category, Subcategory and Login failure reason as description in Windows Security logs.
659018	Minor	Elastic Search	Many phDataManager errors may occur in some situations, caused by FortiSIEM sending malformed JSON to Elastocsearch.
662556	Minor	Event Pulling	AWS CloudTrailParser.xml parses event time incorrectly, which can cause event collection delay.
662540	Minor	Event Pulling	Azure CLI: mLastPollTime is not updated when job failed, causing data collection errors.
662450, 661806, 655562	Minor	Event Pulling	Azure Event Hub event collection errors can cause data collection to stop after running for some time.
660938	Minor	Event Pulling	Guard Duty max count event sometimes does not get picked up.
654551	Minor	Event Pulling	AgentManager can consume memory after running for a while, causing process to stop functioning.
656337	Minor	GUI	Analytics tab - Trend Bar Graph does not show continuity with time and results.
663683, 638773	Minor	Integration	Alienvault STIX OTX Integration may not work for pulling IOCs.
662899	Minor	Parser	Parser function for resolving Hostname to IP address works incorrectly.
659180	Minor	Parser	Collector caches time stamp when rejected from AppServer Check-in.
659171	Minor	Parser	Two events attributes exist with same name Total Connections.
598471	Minor	Parser	Parse MITRE mapping event attributes in Windows Sysmon events.
666962	Minor	App Server	In GUI, Parser > Fix Order function does not work if a specific parser is assigned to a CMDB Device.
666676	Minor	App Server	In SP case, Max number of CMDB Devices for an Organization is not saved.

Bug ID	Severity	Module	Description
660612	Minor	Data	Some system reports do not refer to country name ("United States") instead of "My Home" CMDB Country Group object.
666970	Minor	Event Pulling	AWS CloudTrail can only pull from one region per credential. In new design, FortiSIEM will pull from all regions if the Regions field is left blank.
663934	Minor	GUI	If Slideshow consists of only 1 dashboard, then the slideshow is blank after first refresh.
666755	Minor	Event Pulling	FortiSIEM fails to upload the first startup-config config file to SVN because of incorrect header format. When a change occurs, the files are uploaded.
667091	Minor	App Server	Watch List Query fails in SP environment.
666223	Minor	System	NFS Archive Query may fail sometimes as /archive fails to mount on all Workers during archive set up. Workaround is to delete and then re-add Workers.
666797	Minor	Elasticsearch Support	Some Incident Queries do not run for users with RBAC constrains (e.g. Network Admin).
516477	Enhancement	App Server	Cannot Discover Multiple Devices through Multiple Collectors through API.
665694	Enhancement	Data	The list of public DNS Servers need to be updated.
530467	Enhancement	Device Support	FortiSIEM not detecting certain event SSH/Audit events using UnixParser.
521230	Enhancement	Device Support	Need to support Barracuda F Series Log.
661711	Enhancement	Event Pulling	Parse out SQS log of when Cloudtrail package is logged.
544522	Enhancement	GUI	Cannot delete many credentials at one time.
667032	Enhancement	System	Redis module for charting is unnecessarily turned on in Collectors and Workers. This module is only needed in Supervisor node.

New Device Support

- Tigera Calico - K8 log analysis
- Alcide.io Kubernetes and Microservices Audit log
- Stormshield Network Security

Known Issues

Remediation Steps for CVE-2021-44228

One FortiSIEM module (3rd party ThreatConnect SDK) uses Apache log4j version 2.8 for logging purposes, and hence is vulnerable to the recently discovered Remote Code Execution vulnerability (CVE-2021-44228) in FortiSIEM 5.2.6-5.4.0.

These instructions specify the steps needed to mitigate this vulnerability without upgrading Apache log4j to the latest stable version 2.16 or higher. Actions need to be taken on the Supervisor node only.

On Supervisor Node

1. Logon via SSH as root.
2. Mitigating 3rd party ThreatConnect SDK module:
   a. Delete these log4j jar files under `/opt/glassfish/domains/domain1/applications/phoenix/lib`
      i. log4j-core-2.8.2.jar
      ii. log4j-api-2.8.2.jar
      iii. log4j-slf4j-impl-2.6.1.jar
3. Restart all Java Processes by running: `“killall -9 java”`

FORTINET®