FortiSIEM - Release Notes

Version 5.2.6

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 5.2.6 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
11/19/2019	Initial version of FortiSIEM 5.2.6 Release Notes.
12/16/2021	Added 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 5.2.6 Release.

What's New in 5.2.6

This document describes new and enhanced features for the FortiSIEM 5.2.6 release.

Pre-upgrade notes

1. This release provides an upgrade for all platforms.
2. This release provides Full Install for ESX only. If you want to fresh install 5.2.6 for a platform other than ESX, then follow these steps
   a. Install 5.2.5 for that platform.
   b. Choose the final event database storage: local disk, FortiSIEM EventDB on NFS or Elasticsearch.
   c. Then upgrade to 5.2.6.
3. Previous FortiSIEM releases provided a way for Collectors to download upgrade images from an external website using username and password. If you used this functionality, then Collector upgrade to 5.2.6 may fail. In this case, follow these steps for upgrade:
   If you are running 5.1.2 or earlier:
   a. Clean up Collector Image Server Credentials if still visible from GUI
      i. Go to **ADMIN > General Settings > System > Collector Image Server**
      ii. Delete Username and Password
      iii. Click **Save**
   b. Upgrade Super, Worker(s), Collectors. Note that Collector upgrade can be done from the Supervisor. See Upgrade the Collector Image from the Supervisor in the Upgrade Guide.

   If you are running 5.2.1 or later:
   a. Run the `cleanupdownloadsetting.sql` script - this will clean up the Collector Image Server Credentials if they were set. To run the script:
      i. Log in to FortiSIEM Super
      ii. Download the file from this URL: https://filestore.fortinet.com/docs.fortinet.com/upload/cleanupdownloadsetting.sql and save it in the `/tmp` folder.
      iii. Run this SQL command: `psql -U phoenix -d phoenixdb -f /tmp/cleanupdownloadsetting.sql`.
   b. Upgrade Super, Worker(s), Collectors. Note that Collector upgrade can be done from the Supervisor. See Upgrade the Collector Image from the Supervisor in the Upgrade Guide.
4. If you are running FortiSIEM 5.2.5, then you are familiar with the changes in 5.2.5 - simply follow the regular upgrade process in the Upgrade Guide. Note that Collector upgrade can be done from the Supervisor.

5. If you are running a version of FortiSIEM earlier than 5.2.5, then read the Pre-deployment notes for 5.2.5 first. You can upgrade directly to 5.2.6 but you must be aware of the changes introduced in 5.2.5, for example:
   - The location where you pick up FortiSIEM Images has changed.
   - Elasticsearch query behavior has changed from case-sensitive to case-insensitive.
   - There are special instructions for upgrading Report Server.
   - If you change the GUI Locale, you must reschedule your reports for that Locale.
   - When to add Organizations using Elasticsearch.
   - Redis has changed from running in cluster mode master-slave mode. This is informational.

New Features

This release adds the following features:

Attack Dashboard

MITRE has provided a taxonomy of Security Attack kill chains (https://attack.mitre.org/matrices/enterprise/). In the FortiSIEM 5.2.5 release, MITRE ATT&CK categories were added as FortiSIEM Incident Security subcategories, and FortiSIEM Security Rules were associated with MITRE ATT&CK categories. This release provides a specific Security Incident dashboard, called the Attack Dashboard, that clearly shows the MITRE ATT&CK categories associated with each host based on the triggered incidents. This dashboard enables Security Analysts to quickly focus on hosts that have advanced further in the Attack Kill Chain and mitigate the issues. See Attack View.

Run on Amazon Elasticsearch Service

This release allows FortiSIEM users to enable AWS-managed Elasticsearch (https://aws.amazon.com/elasticsearch-service/). The supported Elasticsearch version is 6.8. See Setting Event Storage.

Collector Upgrade from Supervisor

In FortiSIEM 5.2.5, the user is required to install their own webserver to distribute upgrade images to the Collector nodes. This release simplifies the process by enabling the Supervisor as the webserver. Collectors can download upgrade images from the Supervisor. See Upgrade the Collector Image From the Supervisor in the Upgrade Guide.

Key Enhancements

The following are the key enhancements to the current release:

Show User Roles for AD Group Mappings

Release 5.2.5 allowed FortiSIEM administrators to map Active Directory Groups to FortiSIEM roles. If the user belongs to multiple LDAP groups, then the user is assigned the union of all mapped FortiSIEM roles. A composite FortiSIEM role is not always easy to understand. This release explicitly shows the user's permissions in **CMDB > User > Access Control**. See Viewing User Roles for AD Group Mappings.

Ability to Filter on Any Attribute in Widget Dashboard Search

In FortiSIEM 5.2.5, the user is allowed search for the following attributes in the Widget Dashboard: Host, IP, User, and Device/App Properties. This restriction is relaxed in this release. Now the user can search on any field that appears in at least one widget on a widget dashboard. See Searching in a Widget Dashboard.

Ability to Calculate Much Larger COUNT DISTINCT

In FortiSIEM 5.2.5 and earlier, COUNT DISTINCT queries returned a maximum of 16K. This release extends the number to much higher numbers, using the HyperLogLog algorithm. We have tested up to 1 million with 3% error rate. Higher counts are possible at the expense of higher error rates. See the tables in Creating Rules.

Ability to Download FortiGuard IOC via Proxy

This release allows FortiSIEM to download FortiGuard IOC via a Proxy server (such as Squid) using tunnel mode. See Working With FortiGuard IOCs.

Optimize CASES Tab User Experience

In this release, the CASES tab is displayed in multiple pages, with only one page loading at a time. This makes the CASES page much faster to display. Search is also rendered more efficiently.

New Device Support

The current release includes support for the following devices:

- Cyberoam Firewall
- EPIC EMR/EHR System
- FortiEDR (enSilo)
- FortiNAC
- Microsoft Network Policy Server (RAS VPN)
- Trend Micro Deep Discovery

Important Bug and Data Fixes

All issues listed in Known Issues in Release 5.2.5 have been fixed in 5.2.6.

The current release includes the following bug and data fixes.

- Bug Fixes
- Data Fixes
- Vulnerabilities Fixed

Bug Fixes

The current release includes fixes for these bugs.

ID	Severity	Module	Summary
583870	Minor	App Server	Action history not readable when updating incident attributes through API
529612	Minor	App Server	Users need Admin access to email scheduled reports
545405	Minor	App Server	Malware Domain import from CSV file unnecessarily requires IP address
572905	Minor	App Server	Collector Registration cannot handle "&" or [space] in password
548701	Minor	App Server	Dynamic-reports folder builds up and need to be purged
592278	Minor	App Server	Super attempts outbound connectivity to old images-cdn.fortisiem.fortinet.com site to get updates
592325	Minor	App Server	Only users with Admin privileges can change UI Settings
550599	Minor	App Server	Old Device Maintenance schedules causing high App Server CPU
552111	Minor	App Server	Scheduled report email is sent even if "Do Not Send Scheduled Email if Report is empty" is checked
552712	Minor	App Server	Windows Agent changes device status if already discovered
577845	Minor	App Server	User is not allowed interface if interface mask is discovered as 255.255.255.255
581697	Minor	App Server	Full Admin cannot edit credentials defined by an user
585859	Minor	App Server	REST API: FortiSIEM Agent Status not correct - Disconnected returned as Running Inactive
581924	Minor	App Server	Duplicate device is created if device first discovered by WMI or SNMP and then an Agent is added

ID	Severity	Module	Summary
584853	Minor	App Server	Sometimes unable to run reports caused by database table ph_drq_report_inst not getting cleaned up
584644	Minor	App Server	Agent availability events (Installed/Running/Stopped/Started/Uninstalled/Non-responsive) not being generated
587252	Enhancement	App Server	Integer based attributes do not display the user friendly descriptions in bundle reports
586662	Enhancement	App Server	PH_REPORT_ACTION_STATUS log shows EMAIL database id instead of user name
572872	Minor	GUI	Malware Hash Update from file does not work
470730	Minor	GUI	Rule Exception for Org CMDB report will expose customer information across orgs
575354	Minor	GUI	Dashboard CMDB widget does not map the integer value for "Storage Type" to the corresponding String Value
542982	Minor	GUI	Rule Editor does not properly save expressions in aggregate condition editor after user edits the expression
526824	Minor	GUI	Kafka info is lost after an event forwarding rule via kafka is enabled
568068	Minor	GUI	Analytic Reporting Only shows top 5 results on Trend charts, no matter what rows are checked in the table
513726	Minor	GUI	Storage setup - Testing shows errors if disk is mounted or formatted
582511	Minor	GUI	Unable to add networks to organization if "Include IP/IP Range" is specified Under Org setup
544787	Minor	GUI	Case created due date follows desktop time
576921	Minor	GUI	Windows Agent Host to Template association Rank resets to first page when moving items up the list
512274	Minor	GUI	Event Type Table column headers in Device Support and Resources tabs do not match Analytics Query results
588865	Minor	GUI	Dashboard > Widget Dashboard > Choropleth widget drill down does not show right logs
572875	Minor	GUI	Notification Policy Time Zone Change Reverts back to default when reoccurance has no end date
588712	Minor	GUI	An Org user appears to be able to apply Rule Exceptions to all organizations

ID	Severity	Module	Summary
544011	Minor	GUI	GUI shows large TCP/UDP port numbers as estimated values
583966	Minor	GUI	External Lookup does not pickup IPs from the external lookup request unless you specify <IP> in the URL.
536763	Minor	GUI	Some logged in user on User Activity tab do not show username and role
586077	Minor	GUI	Dashboard drill down does not work correctly for IP Port and Protocol
586546	Minor	GUI	Unable to create ticket from multiple incidents
586640	Minor	GUI	Default Time Range (10 days) on Incident Explorer Dashboard is too long and cannot be modified
582603	Minor	GUI	Widget dashboard > Filters do not appear in some cases
588879	Minor	GUI	Incident > Explorer view pivot on triggering event IP fails
587670	Minor	GUI	Parser clone function sometimes changes two spaces to one space in the parser XML
587473	Minor	GUI	GUI incorrectly showing the subcategory of another rule
593144	Minor	GUI	If there is a rule with undefined sub-category, then Incidents > List View > Search > Categories does not show values
580784	Enhancement	GUI	Make LDAP Group to Role more transparent
586736	Enhancement	GUI	Analytics tab - SAVE and LOAD of Filter/Display tabs are more intuitive
583411	Enhancement	GUI	Content of last column in Tables wraps under the first column
588669	Enhancement	GUI	Not possible to choose Incident Subcategory and Incident Resolution in Custom Email template.
491770	Enhancement	GUI	Login Page lists CUST/ORG ID as part of the login, but takes only Name
585060	Enhancement	GUI	Case management page times out when there are large number of Cases
589991	Enhancement	Linux Agent	Linux Agent to Support CentOS 8+
592736	Enhancement	Linux Agent	FIM does not capture file/directory permission and ownership changes
524355	Minor	Log Pulling	Azure Audit - Stops pulling events but no errors in phoenix.log

ID	Severity	Module	Summary
491789	Minor	Parser/Code	phParser gets stuck against bad CMR records or CDR records -- cannot bypass causing files to back up
575519	Minor	Parser/Code	FortiSIEM does not resolve IP of Fortigates when Fortigate hostname is changed
580645	Minor	Parser/Code	phParser does not support the ability to connect against certificates that have chain certs
597921	Minor	Parser	Windows Defender ATP does not have correct Reporting IP
524276	Minor	Performance Monitoring	Excessive logging: PH_DEV_MON_SYS_STATUS from Meraki
562841	Minor	Performance Monitoring	Fortisiem SSH into fortigate every 3minute though the monitors are disabled
582062	Minor	Query Engine	Elasticsearch queries do not work with network groups with low and high IP addresses specified
582282	Minor	Query Engine	Elasticsearch queries do not work if disable/delete an Malware IP entry from GUI
582145	Minor	Query Engine	Elasticsearch queries do not work for URL IN a single Malware URL item (group works however)
543218	Minor	Query Engine	ReportMaster does not always clean up inline report files
593636	Minor	Query Engine	Queriues containing "Reporting IP IN Biz Service" is not working for Event DB
598441	Major	System	Supervisor Upgrade to 5.2.5 fails when upgrade is performed in the month of December
585536	Minor	System	Swap partition is not created for Super, Worker, and Collector.
586951	Minor	System	RedisCluster_6669 is down after upgrade from 521 to 525 in Elasticsearch based deployments
582939	Enhancement	System	FortiGuard IOC integration is not working via Proxy Server
569343	Minor	System	FortiSIEM Collector doesn't validate Supervisor/Worker HTTPS certificate
519974	Minor	Windows Agent	Not receiving username and domain details for File Integrity monitoring events via Windows Agent. Only fixed for Italian.

Data Fixes

The current release includes fixes for these data and parser/data bugs.

ID	Severity	Module	Summary
528749	Minor	Data	Malware found by Firewall but not remediated references wrong event type group
528725	Enhancement	Data	Additional Office 365 User login succeeded report
535710	Minor	Parser/Data	Wrong user name parseing in FortiGate log cause incorrect Identity and Location dashboard
580973	Enhancement	Parser/Data	AWS VPC doesn't work without accountName
487754	Enhancement	Parser/Data	PAN OS Events parser needs to be enhanced to parse more event types
551006	Enhancement	Parser/Data	Cisco ASA Parser does not parse duration field if time is past 1 day
480346	Enhancement	Parser/Data	Juniper JunOS logs are not parsed because vendor introduced a new format
495878	Enhancement	Parser/Data	Symantec AV - new events are being parsed as symantec av generic
492246	Enhancement	Parser/Data	PAN OS CORRELATION Event not able to be parsed
537118	Enhancement	Parser/Data	FortiGate Parser parse right event type information for LogID(0000000020)
575143	Enhancement	Parser/Data	Meraki Events not parsing all the way -- due to new event types
496607	Enhancement	Parser/Data	FortiMail - not parsing client IP value
492448	Enhancement	Parser/Data	Barracuda Web Filter Parser format change
529083	Enhancement	Parser/Data	Update SymantecAVParser to include log description in event
492489	Enhancement	Parser/Data	SonicOS sonicwall parser needs to be enhanced to parse more event types
493500	Enhancement	Parser/Data	Cisco ASA Parser bug to provide port on pre and post natted events
542444	Enhancement	Parser/Data	Fortisiem not detecting the "lsass" service logs from Ubuntu
576088	Enhancement	Parser/Data	SonicOS parser needd to be updated to include web category
592870	Enhancement	Parser/Data	CloudTrail Parser does not parse account information to an event attribute
549320	Enhancement	Parser/Data	Fortigate Parser Apprisk is not utilizing the correct case

ID	Severity	Module	Summary
556324	Enhancement	Parser/Data	WinOSWmiParser fails to extract attributes correctly on EventCode 4624
557631	Enhancement	Parser/Data	Mysql DB parser does not parse message field completely, due to comma separated values
582689	Enhancement	Parser/Data	If FGT IPS event is denied, dropped, blocked - set event severity to medium
590121	Enhancement	Parser/Data	PulseSecure parser does not handle priority field in syslog header
577186	Enhancement	Parser/Data	BUG - Tipping Point Parser update request
577082	Enhancement	Parser/Data	FortiWeb 6.1.1 Parser Enhancements
576860	Enhancement	Parser/Data	FortiMail parser enhancement, several event attributes not parsed
582975	Enhancement	Parser/Data	SymantecSAPParser need to be extended
575859	Enhancement	Parser/Data	PulseSecure parser needs to be extended
574890	Enhancement	Parser/Data	FortiGate IPS Event Severity needs to be fixed to address firewall action
590127	Enhancement	Parser/Data	FortiOS GTP logs not sufficiently parsed
573605	Enhancement	Parser/Data	Verify FGT Parser is collecting all attributes and update as needed.
573569	Enhancement	Parser/Data	FortiADC logs parser needs to be extended
572910	Enhancement	Parser/Data	PAN firewall parser to support USERID and HIPMATCH events
590451	Enhancement	Parser/Data	Fortigate Parser does not parse Objectpath, Object name, Configuration
570577	Enhancement	Parser/Data	Windows parser to handle escape character when parsing account names
592163	Enhancement	Parser/Data	Office365 Parser does not parse target user field from event
587917	Enhancement	Parser/Data	Incorrect parsing logic in WinOSWmiParser
583269	Enhancement	Parser/Data	User information in GitLab-Authentication-Failure not parsed
582231	Enhancement	Parser/Data	Elasticsearch query does not work with netflow group for FortiGate-NetFlow

Vulnerabilities Fixed

FortiSIEM 5.2.6 is no longer vulnerable to the following CVE-References:

- CVE-2019-17653
- CVE-2019-16153
- CVE-2019-17651

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`"