FortiSIEM - Release Notes

Version 5.3.0

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

12/16/2021
FortiSIEM 5.3.0 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
05/29/2020	Initial version of FortiSIEM 5.3.0 Release Notes.
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 5.3.0 Release.

What's New in 5.3.0

This document describes new and enhanced features for the FortiSIEM 5.3.0 release.

Pre-upgrade notes

- The GUI settings for Archive are lost during the upgrade to 5.3.0. In earlier releases, the user mounted the archive and defined the local mount point in FortiSIEM. In this release, however, the user provides the archive host and exported directory and FortiSIEM performs the mount operation. This action unifies both the online and archive database mounting operations. If you were archiving in version 5.2.8 or earlier, then complete the following steps to recover the archive settings.
    a. Upgrade the Super and all Workers to FortiSIEM version 5.3.0.
    b. Unmount the archive.
    c. Delete the `/etc/fstab` entry of archive setting.
    d. Define the archive in **ADMIN > Setup > > Storage > Archive**. Make sure that the Archive host and exported directories are identical to the settings before the archive.
    e. Click **Test and Save**. FortiSIEM will now archive new events to the same location as before the upgrade.
    f. Delete all of the Workers in **ADMIN > License > Nodes**.
    g. Re-add all of the Workers in **ADMIN > License > Nodes**.

- To remediate a vulnerability in an external module, Flex login via LDAP is disabled.

- Because of changes to the Geo database from release 5.2.x to 5.3.0, some State/Province and City names might not match if they were set for CMDB Devices. For example, the French Province Auvergne in the 5.2.x Geo database changed to Auvergne-Rhone-Alpes in 5.3.0. If you set a device location to Auvergne in 5.2.x, then you must re-edit the location and set it to Auvergne-Rhone-Alpes.

New Features

The 5.3.0 release introduces these key features:

- Search With Display Conditions
- Nested Search
- Use Fortinet GeoIP Database
- Incident Title Using Attributes
- Searchable Archive and Support for HDFS
- Ability to Collect Specific Windows Logs via WMI
- Rule and Scheduled Report Activation Workflow
- Customizable Entity Risk Score for User Selected Rules

Search With Display Conditions

Currently, when you run an aggregated search in FortiSIEM, there is no way to limit the search results. For example, suppose you want to display hosts with an average CPU utilization more than 90%, or users with more than 10 login failures in 1 hour. This release enables you to define display conditions using Boolean logic to limit the search results, just like the HAVING in SQL. This feature works for all supported event databases: FortiSIEM EventDB, Elasticsearch, and HDFS.

For details, see Specifying Search Conditions for Aggregated Search.

Nested Search

This release allows you to use the results of one search in another search using IN or NOT IN operators, just like the SQL Subquery functionality. Suppose you want to show all Servers belonging to a specific Business Service that did not report any login event in last 1 hour - a very useful feature for compliance. To do this, you first define a search that reports all Servers belong to a specific Business Service that sent at least 1 event in last 1 hour. Then, define another CMDB search to exclude the devices in the result of the first search. Another example is to report new Windows/Linux processes for today that were not seen in the last 2 days - a very useful query for threat hunting scenarios.

To accomplish this, this release unifies CMDB and Event searches to be run from the ANALYTICS tab. When you define the filter condition in the outer search, you can specify an attribute IN/ NOT IN the results of the inner search.

Three scenarios are supported:

Outer Query	Inner Query	Use Case
CMDB	Event	Show all servers that did not report any event in the last 1 hour.
Event	Event	Show all successful logins for excessive failed login users. Show new Windows/Linux processes for today that were not seen in the last 2 days
Event	CMDB	Show all failed logins from externally authenticated FortiSIEM admins.

Both FortiSIEM EventDB and Elasticsearch are supported for nested searches. Since Elasticsearch does not natively support nested search functionality, FortiSIEM has built its own nested search functionality on top of Elasticsearch.

Nested searches can be run in adhoc mode from the GUI or can be scheduled. Currently HDFS does not support nested search

For details on how to run a nested search, see Using Nested Queries.

Use Fortinet GeoIP Database

This releases replaces the existing GeoIP database with Fortinet GeoIP database. All of the Geo IP features work in the same way with the new database.

Incident Title Using Attributes

For each rule, you can now define a title containing the incident attributes, for example: “Brute force login from 10.1.1.1 user Bob to Finance Server”. This enables you to quickly summarize an incident without looking into various fields such as Incident Source, Incident Target, and Incident Details. For built-in rules, titles are pre-defined. For custom rules, you must define them after installation. Incident Titles can be used as an Incident attribute in any part of the GUI where an Incident is displayed.

For details on how to define an Incident Title, see Defining an Incident Title.

Searchable Archive and Support for HDFS

When the online event database reaches capacity, events are either purged or archived to make room for new events. The current archive solution has the limitation that one must restore the data from the archive into the online event database – this process is tedious and can consume precious online event database storage. This release enables searching the Archive database from the GUI and also provides two new Archive options for Elasticsearch - FortiSIEM EventDB on NFS and HDFS.

In this release, the following scenarios are supported:

Event DB		Retention		Historical Search		Rules and Real Time Search
Online	**Archive**	**Online**	**Archive**	**Online**	**Archive**	
FortiSIEM EventDB (local or NFS)	NFS	Policy-based and Space-based	Policy-based and Space-based	Super and Workers	Super and Workers	Super and Workers
Elasticsearch	FortiSIEM EventDB (NFS)	Space-based	Policy-based and Space-based	Super and Elasticsearch	Super and Workers	Super and Workers
Elasticsearch	HDFS	Space-based	Space-based	Super and Elasticsearch	Super and Spark Cluster	Super and Workers

The user can set up Archive options from the GUI. For details, see Configuring Storage.

The user can search the Archive event database directly from the FortiSIEM GUI, in the same way as the Online event database. Except for the EventDB scenario, the user can simply choose the event source to be archived in the Filter Dialog.

Ability to Collect Specific Windows Logs via WMI

This release enables you to choose specific Windows (Security, System, and Application) events to be collected via WMI. Choosing only the needed event types enables you to save processing and storage space.

For details on how to collect specific Windows logs via WMI, see Windows WMI Filter.

Rule and Scheduled Report Activation Workflow

Currently any user that has access to the Resources and Analytics tabs can activate a Rule or schedule a Report. A loosely written rule or report can consume serious system resources. This release introduces an audit mechanism in this process via RBAC. The capability to activate a Rule and schedule a report is now part of a Role definition. A user that does not have this capability must request approval and can execute only if approved.

- For details on setting Rule scheduling and Rule activation capabilities as part of a Role, see Adding a New Role.
- For details on Report scheduling using workflows, see Scheduling Reports Using a Workflow.
- For details on Rule activation using workflow, see Activating a Rule Using a Workflow.

Customizable Entity Risk Score for User Selected Rules

This release enables you to choose the rules for the calculation of Entity Risk score. Currently, risk score is based on rules.

For details, see Setting Risk Filters.

Key Enhancements

The 5.3.0 release provides these key enhancements:

- CASE Enhancements
- Agent Based FIM Extensions
- Faster Analytics (Searches, Rules) Using CMDB Objects
- Query Only Workers
- Ability for a Super/Global User to Share Dashboards With Any Organization
- Show Agent License Usage
- Automated CVE-Based Checks for IPS Events
- Incident Dashboard Enhancements
- Widget Dashboard Enhancements
- Custom PDF Enhancements

CASE Enhancements

This release contains several CASE enhancements

- A timeline view to capture activities on a Case and on related incidents.
- A separate Evidence tab is created to capture the attachments and the triggering events.
- Mean Time to Resolution (MTTR) metric for Closed Cases.
- Enhanced search functionality similar to CMDB and Incidents.
- Bi-directional one-click drill down from Incidents to Cases and vice versa.

Agent Based FIM Extensions

This release includes several enhancements for File Integrity Monitoring (FIM) when using Windows and Linux Agents:

- Detect File Permission and Ownership changes.
- Ability to to push monitored files from agents to the FortiSIEM Supervisor where an audit trail of file changes are kept in SVN. The user can then examine the differences between the files.
- Ability to detect file changes from a baseline.

For Windows Agents, see the table of FIM settings in Adding Windows Agent Monitor Templates.

For Linux Agents, see the table of FIM settings in Adding Linux Agent Monitor Templates.

Faster Analytics (Searches, Rules) Using CMDB Objects

In the current architecture, when a search is performed using a CMDB Object, each Worker gets the CMDB Object values from the Supervisor node. The Worker nodes cache the values. When there is a change (for example, caused by discovery or user change), Workers again get the values from the App Server. For a large FortiSIEM cluster with many Worker nodes and large CMDB Objects, the Supervisor’s performance may be impacted, preventing GUI users from logging in.

In this release, Redis distributed database technology is introduced to improve the above performance issue. The Supervisor runs as the Redis Master, while each Worker runs as a Redis Slave. The Supervisor only publishes changes to the Redis Master. Redis rapidly synchronizes CMDB Objects within the FortiSIEM Cluster. The Worker node processes (Rule and Report Workers, etc.) retrieve CMDB Objects from the local Redis, thereby relieving the Supervisor node from providing CMDB Objects from PostGreSQL.

Query Only Workers

This release enables users to have Workers that will only handle Query requests. There are now two types of Worker nodes:

- Query Worker - these worker only handle query requests, adhoc queries from the GUI, and scheduled reports.
- Event Worker - these workers handle all other event processing jobs, including receiving events from Collectors or devices, and storing them into the event database, rule, inline query, real time query, etc.

Reserving Worker nodes for queries allows more system resources to be dedicated to queries and make them run faster.

- For more information on configuring an Event Worker, see Event Worker Settings.
- For more information on configuring a Query Worker, see Query Worker Settings.

Ability for a Super/Global User to Share Dashboards With Any Organization

Currently, a user can share a dashboard only with users belonging to the same organization. Thus, a Super/Global user cannot create shared dashboards with specific Organization users. This release removes this restriction. When Super/Global user shares a dashboard with users of various organizations, FortiSIEM will populate the dashboard with data belonging to specific organizations. Thus, users of a specific Organization will see their own data.

Show Agent License Usage

Users can now see Windows and Linux Agent usage by navigating to **ADMIN > License > Agent Usage**.

Automated CVE-Based Checks for IPS Events

In this release, automated CVE-based checks are performed to detect IPS false positives. If the IPS Events have associated CVEs, but Scanner reports do not show that the target host is not vulnerable to those CVEs, then the Incident severity is downgraded. However, if scanner reports indeed show that the target host is vulnerable to any of those CVEs, then severity is increased and a Case is created.

For more information, see Performing CVE-Based IPS False Positive Analysis.

Incident Dashboard Enhancements

There are several enhancements for **INCIDENTS** tab:

- Ability to save Incident List View Search filters and then load them on demand from a drop down. See Searching Incidents.
- Two additional Incident List Views: List by Device and List by Incidents to facilitate incident investigation. See Viewing Incidents.
- Performance improvement: All the queries under **INCIDENTS** tab, except the Attack View Trend Graph and Trigger event queries, now use data in PostGreSQL database and run faster.

Widget Dashboard Enhancements

There are several enhancements for Widget dashboards in the **DASHBOARD** tab.

- Ability to select all relevant fields in the filter
- Display Bar trend graphs for integer values
- Ability to save column widths for the Table View
- Improved representation in the Donut chart
- Ability to show up to 10K entries in the Table View
- Ability to maximize a widget inline
- Ability to revert color settings for a single line view

Custom PDF Enhancements

- The user can choose to create the PDF in Landscape mode. This provides better readability for table-formatted reports with many columns.
- When a Table is split across more than one page, each page has its own table header for better readability.

New Device Support

The current release includes support for the following devices:

- FortiTester
- Cisco Viptela
- MobileIron
- Duo
- Indegy Industrial Cybersecurity Suite
- Netwrix
- Darktrace DCIP
- Hirschmann SCADA Firewalls and Switches

Existing Device Support Bug Fixes and Enhancements

The current release includes these enhancements for existing devices:

ID	Severity	Summary
616714	Minor	All Account Lockout Rules do not consistently update the Watch List.
611209	Minor	MITRE ATT&CK Categories of a couple of rules are incorrect.
611208	Minor	Phishing attack found but not remediated refers to an incorrect Event Type Group.
610287	Minor	Malware found in a mail rule does not map incident parameters correctly.
605005	Minor	Incident Target is not set for Malware hash match rule.
601979	Minor	FortiGate configuration change events appears under the wrong category.
599966	Minor	JunOS Events appear in the wrong Event Type Group.
598477	Minor	Duplicate Sysmon Event Types appear in the CMDB.
592949	Minor	Windows Application Audit log cleared has incorrect logic.
582647	Minor	Update Snort Signatures.
480266	Minor	No phEventCategory attribute is defined for the PH_SYSTEM_DEVICE_NO_EVENTS event type.
616600	Minor	Enhance Multiple FortiGate Web Filter Log URL Parsing Issues.

ID	Severity	Summary
611928	Minor	High Severity IPS Exploit rule is triggering on denied events instead of permit events.
599406	Minor	Spelling error in Event Type: Win-System-Service-Control-Manager-7045 description in CMDB.
616625	Minor	WinOSWmiParser does not parse DNS Server events coming in through FortiSIEM Windows Agent.
611660	Minor	Sophos XG Firewalls Parser needs enhancement.
610178	Minor	Ironportweb parser needs enhancement to handle new log format.
609981	Minor	SecurityOnionBroParser parser needs updates.
604691	Minor	FortiGate - infoURL is incorrectly parsed.
603930	Minor	Enhance CheckPoint Parser to recognize anti-malware events.
601471	Minor	Fortigate Azure Events are not parsed correctly.
599203	Minor	Meraki Parser does not parse "pattern" for deny or allow.
598691	Minor	Enhance Windows Defender ATP support must be extended to include event types.
598657	Minor	FortiGate VPN/NAT Event has incorrect Event Categories.
598590	Minor	Parse geo location information enhancement from F5 syslog.
598586	Minor	FortiGate Parser enhancement for interface hostname.
597526	Minor	Windows DNS Auditing: there are incorrect and missing Event Types.
596694	Minor	Event Type PAN-IDP-31914 classified as a log on failure, but the vendor does not classify this as a failure.
596569	Minor	SonicOS firewall parser has been fixed to add additional parsing.
596030	Minor	Rule Definition - Event Dropped by License - Value uses peak event drop. It will never stop triggering incidents once started.
595830	Minor	FortiGate parser statically parses "LCD" as a user.
595707	Minor	Watchguard Parser does not parse configuration change event.
594262	Minor	Netscaler Event does not parse the user name and client IP.
594239	Minor	Meraki FW parser does not parse IDS Events.
590452	Minor	Parser incorrectly parses the domain name from FortiSIEM generated host names.
585663	Minor	HuaweiVRPParser -does not parse IP/Port attributes.
580810	Minor	Add Zyxel USG60 FW Event Support.
580645	Minor	When receiving syslog over TLS, the parser does not handle chained certs.
578200	Minor	Some ASA-106010 events are not parsed correctly.
576849	Minor	Certain Palo Alto Networks Firewall Event attributes are not parsed.

ID	Severity	Summary
576099	Minor	Certain Unix logs are not parsed correctly.
575859	Minor	Enhance PulseSecure Parser to handle all syslog headers.
575319	Minor	Windows Correlog parser needs to be extended.
574843	Minor	Windows Detailed DNS Agent Log - destination IP not parsed.
574280	Minor	Need to update WinOSWmiParser.
566111	Minor	SFLOW parser does not pick up all elements in the flow sample.
561293	Minor	JunOS parser sets an incorrect eventAction attribute for RT_FLOW_SESSION_DENY events.
553480	Minor	WinOSWmi parser does not parse MS-SQL login events from an external client.
551497	Minor	RSA Authentication Server draft parser and log samples.
551006	Minor	Cisco ASA parser does not parse duration field if time is past 1 day.
548960	Minor	Enhance MS_OFFICE365_AlertTriggered_Succeeded event to include user and rule.
544277	Minor	Add Support for Symantec Security Analytics Platform.
541957	Minor	Cisco WLC2 parser does not parse user name, SSID , or AP.
521472	Minor	Add support for MikroTik Firewall events.
505270	Minor	Enhance translation for Windows es-CO language.
502441	Minor	Need to parse CLIENT field for MSSQL Events.
493496	Minor	Enhance Bind DNS log parser to include named-sdb.
603560	Minor	Box.com parser does not parse the field ip_address as Source IP.
603129	Minor	JunOS Parser does not parse the user for event type JUNOS_SSHD_LOGIN_FAILED.
592942	Minor	Enhance Windows Sysmon parsing to include more event types.
589900	Minor	Add parser for Azure Event Hub Events.
561431	Minor	Enhance McAfee EPO syslog parser.
555569	Minor	Add CEF syslog format for Trend Micro Apex Central (office scan).
535868	Minor	Add support for Cisco Firepower and NGIPS.
609086	Enhancement	Windows Event parser needs enhancements to parse additional attributes from logs.
607029	Enhancement	Watchguard parser needs enhancement to parse the user from firewall events.
601327	Enhancement	Need ESET Parser to handle JSON formatted events.
597523	Enhancement	SophosWebFilter Parser needs an extension to handle the new event format.
597149	Enhancement	Extend FortiGate Parser to parse more event types.
594189	Enhancement	Office 365 Parser needs some validations for parsing some attributes.

ID	Severity	Summary
579907	Enhancement	Rename winOSParser to an appropriate name like winSyslogParser.
577988	Enhancement	Need to enhance SentinelOne Parser to support for syslog relays.
575277	Enhancement	Enhance Juniper new event type RT_IDP variant.
550100	Enhancement	Enhance Symantec Endpoint Protection parsing.
610632	Enhancement	Enhance IPS rules to include McAfee Stonesoft IPS.
596053	Enhancement	Get OKTA Events with new System Log API.
586639	Enhancement	GitLab Integration: support token authentication.
531794	Enhancement	Need to support Tenable SecurityCenter without Tenable IO.
580253	Enhancement	Cisco IOSXE 5760 WLC cannot discover Access Points.
575002	Enhancement	Support Windows 2019 discovery and performance monitoring.
540965	Enhancement	Oracle Weblogic 12c monitoring fails as it requires the Java client to use wlthint3client.jar.

Other Bug Fixes and Enhancements

The current release includes the following bug fixes and enhancements.

- Bug Fixes
- Other Enhancements

Bug Fixes

The current release includes fixes for these bugs.

ID	Severity	Module	Summary
612884	Major	Analytics	Rule Worker and Query Worker can consume large resident memory under some situations.
616680	Major	Data Purger	Archive Purge may remove more data than necessary because policy check and low disk check run in parallel.
599845	Major	GUI	Online retention policy cannot be saved for Enterprise clients.
617150	Minor	App Server	CMDB Device Update Method becomes MANUAL if the user changes the Device Status from Pending to Approved or vice-versa.
610780	Minor	App Server	The event PH_DEV_MON_LOG_DEVICE_DELAY_HIGH is not generated for LOG only discovered devices.
604530	Minor	App Server	Do not allow REST API to fetch FortiSIEM System Config.

ID	Severity	Module	Summary
599093	Minor	App Server	Windows Performance Monitoring via WMI/SNMP may not work if FortiSIEM Agent is not installed first and reports a new device type that is not recognized by the system.
595355	Minor	App Server	Analytic search queries are not working for certain languages like Korean or Russian.
593726	Minor	App Server	Discovery Modifies "Last Successful" Timer for performance monitoring jobs.
588826	Minor	App Server	Update monitoring through the API is not working.
587796	Minor	App Server	Certificates covering many domains will cause Java SSL connection to throw an error on "hostname does not match".
587458	Minor	App Server	Reports cannot be emailed out to more than 1 CMDB User.
581924	Minor	App Server	Duplicate device is created if the device is first discovered by WMI or SNMP and then the FortiSIEM Windows Agent is added.
571793	Minor	App Server	PH_SYS_COLLECTOR_TRAIL table in postGreSQL becomes too large - need to truncate the table and perform space management.
571480	Minor	App Server	DUO 2FA creates extra users when creating an account for authentication.
555268	Minor	App Server	REST API: Enhancement: Discovery status needs to return the progress percentage.
552712	Minor	App Server	If the agent is installed on top of an approved device, the agent will change the device status to unmanaged --> pending but never back to approved after the template association.
552111	Minor	App Server	An empty report is emailed, even if "Do Not Send Scheduled Email if Report is empty" is checked.
548378	Minor	App Server	AD Group Mapping: if you disable Check Certificate first, then re- enable it, then you need to restart the app server for it to take effect.
524274	Minor	App Server	Scheduled PDF reports emails no longer contain a record count per report.
459758	Minor	App Server	PH_MAX_DEVICES_EXCEEDED reports license is exceeded when the total usage equals but has not yet exceeded the total number of licensed device.
513033	Minor	App Server	Original Device Discovery does not merge the device type after rediscovery because of the lack of a Cisco Generic device type.
613131	Minor	Data Manager	If index_per_customer flag is false, the phDataManager still writes events to different organization's index in Elasticsearch, instead of writing to one index.
608304	Minor	Data Manager	Data purger may consume large amounts of memory even if build_event_statistics=false.

ID	Severity	Module	Summary
594711	Minor	Discovery	LDAP Discovery cannot discover users or groups when DN is configured to lowest level.
593163	Minor	Discovery	For FortiGate via SSH, prompts containing [ ] are not handled.
612698	Minor	Event Pulling	Pulling vulnerability scan reports from Qualys take a long time if there are large number of reports.
612305	Minor	Event Pulling	Crowdstrike API log pulling uses a fixed endpoint firehose.crowdstrike.com even when credential definition points to a different API endpoint.
611979	Minor	Event Pulling	FortiGuard IOC update via proxy fails when the Supervisor cannot resolve the FortiGuard endpoint.
610179	Minor	Event Pulling	Tenable Security Center can support only one account.
605231	Minor	Event Pulling	Any device credential without a user name, password or apiToken can cause some back end modules to crash.
603118	Minor	Event Pulling	Incorrect FireSight Error message, "unable to get certificate", displays for possible password failures.
571470	Minor	Event Pulling	FortiSIEM suddenly stops collecting events from CheckPoint SmartCenter.
497122	Minor	Event Pulling	Missing memory Name attribute for PH_DEV_MON_SYS_MEM_UTIL event.
616673	Minor	GUI	Browser memory grows very fast when running Dashboard Slideshow.
612256	Minor	GUI	User is allowed to query events with Equal operator and multiple values.
610750	Minor	GUI	If you click run for 37+ organizations in the Dashboard widget, the configuration will not save.
609498	Minor	GUI	Pressing ENTER key in the Rule or Report Description will result in a SPACE and not a line return.
606710	Minor	GUI	Auto refresh on Incident Overview tab is not working in Fortisiem 5.2.5 and 5.2.6.
606092	Minor	GUI	CMDB Report does not report the Last Domain Logon and Password Last Set Values correctly.
600202	Minor	GUI	User cannot add user created business service groups to Settings > Discovery > CMDB Groups.
596814	Minor	GUI	Enabled parsers may not be distributed to workers.
595760	Minor	GUI	Event Type Search for PH_DEV_MON_NET_ shows NETAPP events.
595401	Minor	GUI	Malware hash IOC import via the CSV file requires the botnet name -- the hash should be enough
595214	Minor	GUI	Enterprise /online retention policy saved as "all organizations". There is

ID	Severity	Module	Summary
			no option to change.
595186	Minor	GUI	If the user disables Online Retention Policy, then the information is not saved in the database.
594437	Minor	GUI	New Resources > Default Password for SNMP requires a User Name.
593644	Minor	GUI	Incident Display Column changes are applied "per org" instead of "per user".
591648	Minor	GUI	Parser test does not show message value in HTML5 but shows in Flex.
589908	Minor	GUI	User sees "No Write Permission" when editing their own password, but password changes anyway.
588863	Minor	GUI	Windows Agent CMDB Display Inconsistencies - Method column does not display AGENT if the server has also been discovered by WMI; Status column behavior is incorrect when the agent is disabled then re-enabled.
588846	Minor	GUI	The "Run as Query" button does not populate filter conditions in the analytics page if the rule has more than seven filter conditions.
587919	Minor	GUI	If you set the Target of a CMDB Report to "Report", it displays the Rule Category field.
587346	Minor	GUI	User cannot choose Scatter plot "Size" attribute to be anything other than the X or Y attribute. A third attribute is the main use case.
587092	Minor	GUI	Super/Local Licensed Count shows unallocated device count.
582511	Minor	GUI	Unable to add networks to an organization if "Include IP/IP Range" is specified under Org setup.
575582	Minor	GUI	Organization Name does not display in a Report unless the Organization ID is also in the Report.
572878	Minor	GUI	Install Patches "installed time" does not display in HTML5, but is available and reflected in flex for the same device.
572867	Minor	GUI	GUI does not render with readable columns under CMDB > Devices > Quick Info.
563711	Minor	GUI	When viewing the page on a larger, external monitor, the UI does not display the data in the last column.
552721	Minor	GUI	Pull Events / Discovery tabs display "Discovered by supervisor". It is actually a list of all enterprise devices only.
498942	Minor	GUI	If Built in Admin User from an organization is removed, FortiSIEM picks up a random full admin to be organization administrator. The user should never be able to delete the Built in Admin User.
479356	Minor	GUI	Users should not be able to choose themselves as the manager on H5.
475953	Minor	GUI	External Lookup for Domain is grayed out.

ID	Severity	Module	Summary
609243	Minor	GUI	RegEx filtering with "\" produces an Extra "\" after the expression is saved.
587670	Minor	GUI	In the cloned parser XML, two spaces are changed to one in some xml functions.
599215	Minor	Identity location	In certain cases with multi- tenant collectors, Identity and Location Report for one organization may display data for another organization.
541960	Minor	Performance Monitoring	Large disks are not monitored correctly for utilization using SNMP.
498682	Minor	Performance Monitoring	River Bed Peer monitoring fails.
540487	Minor	Performance Monitoring	ASR 9k large memory capacity router reports 100% memory usage.
604928	Minor	Query	Operators HourOfDay and DayOfWeek are not working when using Elasticsearch.
582062	Minor	Query	Elasticsearch query does not work with network groups with low and high values.
620383	Minor	Query	Elasticsearch scrolled queries cause the Elasticsearch node to run out of memory.
620428	Minor	Query	The Elasticsearch index sends fail messages because the utf8 characters in events are not escaped the first time.
626036	Minor	Query	The ElasticSearch precision_threshold causes the Elasticsearch node to run out of memory on COUNT DISTINCT queries.
563753	Minor	VULN	FortiSIEM should force users to change default password on first time GUI/CLI login.
557076	Minor	VULN	jQuery 1 has a new CVE, CVE-2019-11358 disclosed on 2019-04-19.

Other Enhancements

The current release includes these enhancements:

ID	Severity	Module	Summary
609317	Enhancement	App Server	Setting PHOENIX_MERGE_BY_HOSTNAME_ONLY attribute in phoenix_config.txt to true results in duplicate devices.
600891	Enhancement	App Server	Allow super global user to share a dashboard with any user.
579895	Enhancement	App Server	Merging message is misleading when not merging based on IP.
544876	Enhancement	App Server	Long tables spanning multiple pages in PDF Report Export need to be broken up into multiple tables with their own headers.

ID	Severity	Module	Summary
509857	Enhancement	App Server	Landscape mode is needed to print tables with many columns in PDF report.
477152	Enhancement	App Server	Add Audit logs for FortiSIEM user role change.
434850	Enhancement	App Server	Use Vulnerabilities reported against devices with IPS Events to determine attack success.
616057	Enhancement	Data Purger	Separate thresholds for online and archive.
591511	Enhancement	Event Pulling	FortiSIEM needs to use "show running-config view full" command over SSH to collect configuration.
609828	Enhancement	GUI	Need to allowIP ranges when setting up Virtual IPs used for CMDB Device merging.
601457	Enhancement	GUI	Show the root cause of the Sudden Login Distribution Change rule with a visual chart.
582246	Enhancement	GUI	User cannot create a new object easily without pointing to a group first.
573534	Enhancement	GUI	FortiSIEM GUI sends the login name and password in plain text inside HTTP(S). GUI needs to hash the password.
559179	Enhancement	GUI	Ability to assign an Incident to "In Progress".
552984	Enhancement	GUI	PDF export does not have columns sized correctly when there are too many columns.
497502	Enhancement	GUI	Tunnel pop up vanishes too quickly, needs to have confirmation button.
609469	Enhancement	H5_Admin	Event Org Mapping with Reporting IP as the event attribute does not allow a comma separated IP list.
609166	Enhancement	Performance Monitoring	Restore Job stat logs in DEBUG mode.
617283	Enhancement	System	Tune Linux socket buffers and socket listen queue to higher values to accommodate both large and small customers.
608249	Enhancement	System	Add "Query Only" Worker List to only perform Queries.

New Reports

The following reports are new for this release:

- FIM Reports
- Audit Reports

FIM Reports

- Agent FIM: Windows File/Directory Created/Deleted/Renamed
- Agent FIM: Windows File/Directory Ownership Changes
- Agent FIM: Windows File/Directory Permission Changes
- Agent FIM: Windows File/Directory Archive Bit Changes
- Agent FIM: Windows File Content Modified in SVN
- Agent FIM: Windows File Content Modified
- Agent FIM: Windows File Change from Baseline
- Agent FIM: Linux File/Directory Creation/Deletion/Movement/Unmount Activity
- Agent FIM: Linux File/Directory Ownership or Permission Changes
- Agent FIM: Linux ASCII File Content Modification
- Agent FIM: Linux File Content Modified
- Agent FIM: Linux File Change from Baseline
- Agent FIM: Linux File Content Modified in SVN

Audit Reports

- FortiSIEM CMDB Device Addition via Discovery
- FortiSIEM CMDB Device Addition/Deletion By User
- FortiSIEM CMDB Device Modification via Discovery
- FortiSIEM Device Modifications
- FortiSIEM CMDB Device Discovery Merge History
- FortiSIEM Scheduled Malware IOC Update History
- FortiSIEM Admin User Added
- FortiSIEM Admin User Deleted
- FortiSIEM Admin User Password Modified
- FortiSIEM User Default Role Changed
- FortiSIEM User Organization Role Enabled/Disabled/Changed
- FortiSIEM Role Created/Deleted
- FortiSIEM SSH Tunnel Open/Close History
- FortiSIEM User Initiated Performance Monitoring Job Status Changes
- FortiSIEM Discovery Removed/Not-scheduled Performance Monitoring Jobs
- FortiSIEM Performance Monitoring Job Execution Failures
- FortiSIEM CMDB Device Status Changes
- FortiSIEM Device License exceeded - Device Set to Unmanaged
- FortiSIEM Rule Activation Approval Activity
- FortiSIEM Rule Deactivation Approval Activity
- FortiSIEM Report Schedule Approval Activity
- FortiSIEM CMDB Device Added or Deleted
- FortiSIEM CMDB Device Status Change
- FortiSIEM Rule Added/Deleted
- FortiSIEM Rule Modified
- FortiSIEM Report Added/Deleted

- FortiSIEM Report Modified
- FortiSIEM Rule Activated/Deactivated
- FortiSIEM Reports Completed
- FortiSIEM Reports Scheduled
- FortiSIEM Reports Stopped
- Slowest FortiSIEM Event Reports
- FortiSIEM Dashboard Folder Added/Deleted
- FortiSIEM Dashboard Folder Shared
- FortiSIEM Incident Notification Policy Added/Deleted
- FortiSIEM Incident Notification Policy Executed
- FortiSIEM CMDB Discovery Execution
- FortiSIEM On-demand Remediation Executed
- FortiSIEM Case Created/Updated/Closed
- FortiSIEM Incident Cleared By User
- FortiSIEM Incident Cleared By System
- Successful Online Event Database Archive Actions
- Successful Online Event Database Purge Actions
- Successful Archive Event Database Purge Actions
- Successful Archive EventDB Policy-based-Purge Actions
- Successful Archive EventDB Low-Space-Purge Actions
- Failed Event Database Archive or Purge Actions

New/Modified Rules

The following rules are new or have been modified for this release:

- Lateral Movement Detected
- Agent FIM - Linux File Content Modified
- Agentless FIM - Audited file or directory created
- Agentless FIM - Audited file or directory deleted
- Agentless FIM - Audited file or directory ownership or permission changed
- Audited file or directory content modified in SVN
- Agentless FIM - Audited target file content modified
- Agent FIM - Linux File Ownership or Permission Changed
- Agent FIM - Linux Directory Ownership or Permission Changed
- Agent FIM - Windows File or Directory Created
- Agent FIM - Windows File or Directory Deleted
- Agent FIM - Linux File or Directory Created
- Agent FIM - Linux File or Directory Deleted
- Agent FIM - Windows File Content Modified
- Agent FIM - Windows File Permission Changed
- Agent FIM - Windows File Ownership Changed
- Agent FIM - Windows File or Directory Archive Bit Changed
- Agent FIM - Windows File Changed From Baseline

- Agent FIM - Linux File Changed From Baseline
- FortiSIEM Online Event Database Archiving Failed
- FortiSIEM Archive Directory Unavailable
- FortiSIEM Online Event Database Archiving Completed
- FortiSIEM Online Event Database Successfully Purged
- Low Available System Archive Space
- FortiSIEM Archive Event Database Purging Started
- FortiSIEM Archive Purging Completed
- FortiSIEM Archive Purging Failed

Vulnerabilities Fixed

FortiSIEM 5.3.0 is no longer vulnerable to the following CVE-Reference:

- CVE-2015-0279

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”`