High Performance Network Security

FortiSIEM Release Notes

Version 5.2.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://fortiguard.com/

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

FORTINET®

9/3/2019

FortiSIEM - 5.2.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-03-15	Initial version of FortiSIEM 5.2.1 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 5.2.1 Release.

What’s New in 5.2.1

Pre-deployment considerations

Release 5.2.1 includes significant changes in many areas. Consider the following before you deploy fresh or upgrade to 5.2.1.

1. To address security vulnerabilities with lighttpd port 5480, Collectors cannot be registered to Supervisor via GUI. Instead, Collectors need to be registered by running this script:
   ```
   phProvisionCollector --add <user> <password> <super IP or
   host> <organization> <collectorName>
   ```
   See Security hardening for details.
2. FortiSIEM Windows and Linux Agent architectures have changed significantly:

- Windows Agent 3.1 released first with FortiSIEM 5.2.1 do not need and will not work with Windows Agent Manager.
- Linux Agents now need to be licensed. Both Windows and Linux agents will contribute towards the Agent license: *SKU GSM-AGT-ADV-XXX-UG*
- Windows and Linux Agents need to be configured from the Supervisor.
- Windows Agents 2.2 and earlier will not work with FortiSIEM 5.2.1 and later. You need to install new Windows Agents 3.1.
- Older Linux Agents (LinuxFileMon) can work as it sends syslog to FortiSIEM 5.2.1. We recommend using the new Linux Agent 5.2.1.

3. Selenium based Synthetic Transaction Monitoring will not work out of the box, since Google Chrome packages have security vulnerabilities and have been removed. Fixes for Google Chrome compatible with CentOS6 are not available. Do not upgrade to 5.2.1 if you need Selenium based Synthetic Transaction Monitoring.
4. FortiSIEM Disaster Recovery and Failover require PostgreSQL database to be upgraded to 9.4-BDR. Therefore, 5.2.1 upgrade will take relatively longer duration to complete, as data has to be migrated out and then imported back.
5. FortiSIEM 5.2.1 now supports Elasticsearch 6.4.2. In addition, at least 1 Hot Data Node is required if there is no replication and at least 2 Data Nodes for 1 Replication. If you are running any earlier version of FortiSIEM and Elasticsearch 5.6.2, follow the upgrade documents carefully to first upgrade FortiSIEM and then upgrade Elasticsearch. Note that FortiSIEM 5.2.1 works with older Elasticsearch 5.6.2 as well. *See Elasticsearch Storage Guide here for details.*

FortiSIEM 5.2.1 release includes the following:

- New Features
- Enhancements
- New Device Support
- Device Support Enhancements
- Resolved Issues

New Features

FortiSIEM 5.2.1 release includes the following new features:

- Automated Failover and Disaster Recovery
- Multi-tenant Collectors
- Data Anonymization support
- Windows Agent without Windows Agent Manager
- Linux Agent
- Custom Log File Analysis
- PCI Logging Status Dashboard
- Packet Capture (PCAP) File analysis
- Ability to forward any event in FortiSIEM to an external server via CEF
- Azure Platform Support

Enhancements

FortiSIEM 5.2.1 release includes the following enhancements:

- Elasticsearch deployment and performance enhancements
- Windows Agent enhancements
- HTML GUI enhancements
- Ability to rate limit collectors
- Rule Worker Performance optimization
- Incident Reporting status
- Case Management enhancements
- Custom Device Property support in Analytics
- System Security Hardening

New Device Support

- AWS Cloud Passage Halo - log collection via API
- Tenable.io (new) - log collection via API
- GitLab (new) - log collection via API
- Rapid7 InsightVM - log collection via API
- Crowdstrike - log collection via Streaming API, Data Replicator
- Sophos Central - log collection via API
- Windows Defender ATP - log collection via API
- Tanium Connect - log parser
- OneIdentity - log parser

- Cyxtera AppGate - log parser
- PacketFence - log parser
- Cimcor CimTrak - log parser
- Watchguard Firebox - discovery and performance monitoring
- TruStar - Threat Intelligence integration via API
- ThreatConnect - Threat Intelligence integration via API

Device Support Enhancements

- Microsoft Office365 - new event types
- ForeScout CounterACT - enhanced log parser
- AlertLogic - enhanced log parser
- Cisco ISE - enhanced log parser
- Box - API - log collection
- Nessus Pro v7 and v8
- McAfee EPO - enhanced log parsing
- FortiManager - enhanced syslog parsing
- PulseSecure - enhanced syslog parsing
- Digital Guardian DLP - enhanced syslog parsing
- HP ComWare - enhanced syslog parsing
- F5 LTM - enhanced syslog parsing
- Office 365 - enhanced management activity log parsing
- Checkpoint Firewall 1 - CEF and syslog event parsing
- Windows - French language - enhanced security event parsing
- FireAMP/eStreamer - new agent

Automated Failover and Disaster Recovery

This release enables native FortiSIEM Failover and Disaster Recovery. The feature works with all FortiSIEM deployments – hardware appliance, all-in-one Virtual Appliance and Super/Worker Cluster using NFS based Event Database (Event DB) or Elasticsearch.

This feature enables customers to have two FortiSIEM systems – one Primary FortiSIEM for full Read/Write operations and a Secondary FortiSIEM for Read only operations. Logs are sent to the Primary Site. Discovery and Performance monitoring happens on the Primary Site. Users normally login to the Primary Site. Alerts and notifications trigger on the Primary Site. The full state - CMDB (PostGreSQL DB), Config (SVN), Profile data (SQLite DB) and Event DB (NFS based Event DB or Elasticsearch) are synched from Primary to Secondary – are synched from the Primary to the Secondary. Users can login to the Secondary FortiSIEM and run searches – the results are available after a slight delay.

After disaster, the Secondary FortiSIEM can become the Primary and users and events can be diverted to the new Primary using DNS mechanisms.

This feature requires a separate FortiSIEM license with exactly same parameters as the original. FortiSIEM has to be set up in two sites in an identical fashion, implying identical number of Super, Workers and identical Event

DB (NFS or Elasticsearch) at the two sites. To handle CMDB replication, the embedded PostgresSQL database will be automatically upgraded to 9.4-BDR as part of 5.2.1 upgrade.

For details about setting up Failover and Disaster Recovery, see here.

Multi-tenant Collectors

A Collector is an important component in a multi-tenant FortiSIEM deployment. By associating one or more Collectors to an Organization, devices and logs can be easily associated to that Organization.

Prior to 5.2.1, Collectors can be deployed in one of two ways:

- **Many-to-One deployment**: Collectors can be associated to an Organization in many-to-one fashion. Logs collected and devices monitored by a Collector belong to the corresponding Organization.
- **Special One-to-Many deployment**: To handle multi-tenant log sources (for example, FortiGate firewall with VDOM), a Collector can be associated to the special Super/Local FortiSIEM Organization. You can define Event Organization Mapping Rules to map the Organizations in multi-tenant devices to FortiSIEM Organizations. The Collector uses the Event Organization Mapping Rules to associate devices and logs to the correct FortiSIEM Organization.

A Collector belonging to the Super/Local Organization is a multi-tenant Collector, since it can handle multiple Organizations. In this release, the multi-tenant Collector concept is enhanced further:

- **Multi-tenant Agents**: FortiSIEM Windows Agent 3.1 and Linux Agents 5.2.1 belonging to any Organization can send logs to a multi-tenant Collector. Using the Organization Id information in log, a multi-tenant Collector can associate the Agents and the logs to the correct Organization.
- **Multi-tenant Event Pulling**: When events need to be collected via an API (for example, AWS Audit trail), the user can now associate a FortiSIEM Organization to a credential. The event collection job is assigned to a multi-tenant Collector and it associates events to the correct Organization.
- **Multi-tenant Collector Pool**: For scalability, multiple multi-tenant Collectors can be defined for the Super/Local Organization. Windows and Linux Agents send to the multi-tenant Collector pool in a round-robin fashion. API based event pulling jobs are distributed by the Application Server to a collector from the multi-tenant collector pool. If one Collector goes offline or is deleted, the job is automatically re-distributed to another multi-tenant Collector.

For details about various deployment scenarios, see here.

For details about setting up multi-tenant collectors, see here.

Data Anonymization Support

Starting this release, FortiSIEM can anonymize any parsed log field containing Personally Identifiable Information (PII), including IP addresses, host names, user names, MAC addresses and email addresses. User can choose any attribute including custom-defined attributes for anonymization. This enables Organizations to comply with data privacy regulations such as General Data Protection Regulation (GDPR).

Anonymization is done for externally received logs, internally generated logs, incidents and CMDB records, search results, notifications. FortiSIEM is able to store the event database on both NFS and Elasticsearch deployments. Encryption can be used where the underlying storage is encrypted by the external storage system in a way that is transparent to FortiSIEM. If the user mounts the hard disk at a different location, a password is required to access the internal data.

Data Anonymization is role-based. You need to define a new role, specify the attributes to be anonymized for that role and map users to that role. FortiSIEM includes a de-anonymization workflow. You need to define a de-anonymization approver user for approving de-anonymization requests. A user may create a de-anonymization request. Once the request is approved for a specific time duration, the data is de-anonymized for the specific user and duration. After the de-anonymization duration expires, the date is re-anonymized using a different key.

Currently, a user belonging to the anonymized role has the following restrictions:

- User cannot see any part of the raw events – they are completely hidden.
- User cannot perform search on anonymized event attributes.
- User cannot run CSV exports on search results.
- If an integer event field is anonymized, the GUI may not show those fields. Normally, integer fields are not anonymized.

For details about setting up data anonymization support, see here.

Windows Agent without Agent Managers

Windows Agents (version 3.1 onwards) can now be centrally configured and managed from the FortiSIEM GUI. Windows Agent Manager is not required.

Note: Collectors are required to collect logs from Windows Agents.

The new Agent configuration process is similar to earlier releases, except that it is done from FortiSIEM GUI and can be applied globally to Agents belonging to multiple Organizations in Service Provider deployments.

a. Define Windows Monitoring Templates in GUI
b. Associate Windows hosts to Monitoring Templates and a list of Collectors.
c. Deploy the Agents.

Agents register to Supervisor and obtain the respective monitoring templates and the list of Collectors to forward events. Agents collect logs according to the monitoring template and send to one of the available Collectors. If any change is made to the template or the Collector list, the changes are propagated to the Agents. Agents can send logs to a different Collector from the list, if one is busy.

The new centralized Agent configuration approach simplifies Agent management and eliminates the need to have an Agent Manager. In addition to providing the same functionality as earlier 2.x versions, new Agents include additional features as described in the Windows Agent Enhancements.

For details about setting up Windows 3.1 agents, see here.

Linux Agents

This release introduces Linux Agents (Version 5.2.1) with the following functionalities:

- Collect any logs sent to the syslog facility
- Monitor Custom log files
- File Integrity Monitoring

Note: Collectors are required to collect logs from Windows Agents.

Linux Agents configuration is done from FortiSIEM GUI and can be applied globally to Agents belonging to multiple Organizations in Service Provider deployments.

a. Define Linux Monitoring Templates.
b. Associate Linux hosts to Monitoring Templates and a list of Collectors.

c. Deploy the Agents.

Agents register to Supervisor and obtain the respective monitoring templates and the list of Collectors to forward events to. Agents collect logs according to the monitoring template and send to one of the available Collectors. If any change is made to the template or the Collector list, the changes are propagated to the Agents. Agents can send logs to a different Collector from the list, if one is busy.

Linux agents need to be licensed in the same way as Windows Agents. FortiSIEM enforces the total number of Windows or Linux Agents deployed within the system.

For details about setting up Linux 5.2.1 agents, see here.

Custom CSV File Analysis

This release allows the ability to load a custom CSV file from the GUI. User can define a mapping from CSV file columns to event attributes. FortiSIEM will generate events – one for every line in the log file. The events can be searched like an externally received event.

For details about setting up a custom CSV file for analysis, see here.

PCI Logging Status Dashboard

This release provides a dashboard that provides a status of PCI devices that are logging/not logging at all or logging correctly. Logging correctness is defined on a device group basis by associating a Report to a device group in Report > Compliance folder.

For details about setting up PCI Logging Status Dashboard, see here.

Azure Platform support

FortiSIEM can now be deployed in Azure Clouds.

For more information about FortiSIEM Azure Collector installation, see here.

PCAP File Analysis

This release allows user to parse PCAP files. IP, TCP/UDP and HTTP attributes. PCAP files can be moved to this location on any node defined in `phoenix_config.txt`.

Ability to forward any event to an external server via CEF

This release enables FortiSIEM to forward logs to an external system using Common Event Format (CEF) format over UDP or TCP.

For details about setting up event forwarding via CEF, see here.

FortiSIEM parsed event attribute to CEF attribute mapping is defined here.

Elasticsearch deployment and performance enhancements

FortiSIEM can be configured to use Elasticsearch as its event database – this enables FortiSIEM to scale out event storage and search capabilities using Elasticsearch distributed architecture. This release adds the following

Elasticsearch related enhancements:

- Elasticsearch 6.4.2 version support.
- Multiple Coordinator node support for fail-over: Enter multiple coordinator nodes using a comma separated manner in **Admin** > **Setup** > **Storage**.
- **Ability to store events on per-customer basis in Service Provide deployments**
  For multi-tenant deployments, you can optionally store logs for each Organization in a separate Elasticsearch index. This enables you to easily delete the logs for an Organization if needed, without affecting the performance of the system.

  To do this set `index_per_customer = true` in the Elasticsearch section of `/opt/config/phoenix_config.txt` for Super and each Worker nodes.

  ```
  [BEGIN Elasticsearch]
   enable=false
   ...
   index_per_customer=false
   ...
  [END]
  ```

  By default, `index_per_customer = false`

  It is highly recommended to set this at the beginning of the install before events are stored in Elasticsearch. Once the setting is changed, Supervisor and Worker nodes need to be restarted for the modules to read the change. If the change is done after Elasticsearch has been running for a while, then the queries around the time of change may not work properly. But queries for time window before or after the time change will work correctly.

  Note: You will likely need more data nodes if you decide to separate customer data. Refer to the Elasticsearch capacity planning guide.
- **Elasticsearch log storage capacity improvements**
  a. Use 'best compression'.
  b. FortiSIEM event attribute types mapped to the smallest (in size) Elasticsearch data type.
  c. FortiSIEM profile data and per-Worker-5minute-inline-report data not stored in Elasticsearch.
  d. Option to not store inline report data in Elasticsearch. Inline reports speed up Dashboard display. There are now three options to choose from:
     i. **Disable inline computation** – when the user visits a Dashboard, the GUI will query directly raw events in Elasticsearch – this does not consume Elasticsearch storage.
     ii. **Inline computation via files** – inline computation is still done but the results are stored in files on Supervisor node - this does not consume Elasticsearch storage. This approach is the same as FortiSIEM NFS based Event Database.
     iii. **Inline computation via Elasticsearch (default)** – Inline computation results will be stored in Elasticsearch. It consumes Elasticsearch storage and dashboard will load faster. However, compared to earlier releases, per Worker results are not stored and merging is done outside of Elasticsearch – so Dashboard queries will be equally fast but consume less space.
- **Support of tiered Elasticsearch Hot/Warm storage**

  User can configure certain Elasticsearch Data Nodes (typically with SSD) as Hot Nodes, and remaining Data Nodes (typically with magnetic disks) as Warm Nodes. In this configuration, read/writes involving recent logs go to the Elasticsearch hot nodes. When the hot nodes become close to full, then logs are migrated to Warm nodes. When the Warm nodes become full, logs are either Archived (if an archive destination is defined) or purged. FortiSIEM manages the Hot > Warm > Archive data movement based on user defined storage utilization thresholds. User can search events from Hot and Warm nodes in a transparent manner – specific knowledge of data residence is not needed. Currently, restore from Archived node to Elasticsearch Warm nodes is not supported.

- **Support of CMDBDeviceToAttributeMap functionality in Elasticsearch searches**
  Often there is a need to 'join' log data with device properties from CMDB. The `CMDBDeviceToAttributeMap` function provides this functionality with custom device properties. These searches now work for Elasticsearch.

Windows Agent Enhancements

This release contains the following Windows Agent specific enhancements, in addition to the ability to work without Agent Manager functionality described earlier.

- **Support for Windows Event Forwarding**

  Windows can forward logs using Windows mechanisms to a Central Windows Server. A FortiSIEM agent on the central server can then bring all the events from the various windows servers to FortiSIEM. This is an alternative to running FortiSIEM agent on every Windows server. The disadvantage of this approach is that Windows (Security, application and system) event logs can be collected in this way, while FortiSIEM agent can collect other information such as FIM, Custom log, Sysmon etc. This release is able to parse the forwarded Windows events so that actual reporting Windows server is captured and all the attributes are parsed as sent by native agents.
- **Support of Windows FIPS enabled mode**

  In earlier releases, the agent did not work properly if FIPS mode was turned on. This issue is addressed in this release.
- **File hash for File Integrity Monitoring computed using SHA256**

  The file hash value for file/folder monitoring is now reported using SHA256 algorithm instead of MD5. This enables direct match with external threat intelligence malware file hashes.

For enabling Windows Event Forwarding on Windows Servers, see here.

For enabling FIPS on Windows Servers, see here.

HTML GUI Enhancements

This release adds the following important GUI enhancements:

- Light theme is now added for FortiSIEM GUI. This can be configured on a per user basis under **ADMIN** > **Settings** > **System** > **UI**.
- User state is saved while the user navigates from one tab to another during a login session. When the user goes back to a tab, the last user view is shown.

- The following items are added from Flash GUI:
  - Dashboard slide show
  - Interface Usage Dashboard
  - Event Database Management – works both for NFS based Event Database and Elasticsearch
  - Port Mapping table
  - Application Health table
- Keyword-based search is added in Analytics.
- User can save the Analytics Filters and Time Range attributes and then choose the Saved Filters in Search later.
- Dashboard search filter GUI is redesigned to be similar to Incident Search.
- When user creates a Dashboard Search, queries are run on-demand to capture all data.
- SNMP SysObject Ids can be defined from GUI. This enables custom device discovery.
- New Dashboard view with counts of important types in CMDB and Case tabs.
- New main 'TASK' tab for managing de-anonymization approval and requests.

For setting light theme, see here.

For creating Dashboard slide show, see here.

For creating Interface Usage Dashboard, see here.

For details about Event Database Management, see here.

For Keyword based search, see here.

For saving and displaying Analytics Filters and Display attributes, see here.

For creating SNMP SysObject Ids, see here.

For details about de-anonymization, see here.

Ability to Rate Limit Collectors

This release allows user to limit the rate at which Collectors can send events to Workers.

FortiSIEM, being a real-time event correlation system, requires Collectors to push events as quickly as possible to the Workers. However, if Collectors are offline for a long period of time or Internet bandwidth is scarce, then the Collector to Worker link can get overwhelmed. By defining an upper limit on a Collector bandwidth, the user can force the Collector to limit Collector to Worker bandwidth usage. Note that the drawback of rate limiting is that events may be delayed and correlation rules may not trigger for the delayed events. Also, events may get lost if Collector disk gets full if Collector is receiving events at a higher rate than it is allowed to send.

For setting an upper limit on a Collector bandwidth, see here.

Rule Worker Performance Optimization

In this release, the Rule Worker CPU performance is improved by keeping a cache of event type to Rule mappings – this eliminates the requirement to check every rule for event type match.

Incident Reporting Status

This release adds the incident reporting device status flag (Approved or Pending) to every incident. This enables users to quickly identify the incidents triggered by Approved devices and assign them higher priority.

Case Management Enhancements

This release adds several enhancements to the in-built Case management system:

- Ability to search cases using Incident Id.
- Ability to drill down from Case to Incident List view page with the incidents pre-selected.
- Display the triggered events directly in a Case.

For more information about Case Management, see here.

Custom Device Property Support in Analytics

This release allows users to define custom device properties and then display them under CMDB for use in Analytics searches and incidents.

System Security Hardening

In this release, FortiSIEM Super, Worker and Collector system is configured to be more secure. Following are the Security Hardening enhancements in various ports:

Port 443 hardening

- Removed Apache default installation/welcome page.
- Disabled HTTP OPTIONS method.
- Allows only TLS 1.2 and good ciphers: AES128-SHA, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384.

Port 21 hardening

- Allows only TLS 1.2 and good ciphers: AES128-SHA, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384.
- Disallows non-SSL FTP.

General system hardening

- Google Chrome packages are removed - so Selenium based Synthetic Transaction Monitoring will not work out of the box.
- ICMP redirection is disabled.
- Only root partition allows device files (Partition mounting weakness).
- TCP timestamp response is disabled.
- Tightened permission for user nfsnobody (used for nfs mounting).
- Removed Ghostscript package.
- Changed permission of some files from world writable to world readable.
- All path entries are made absolute paths.

Port 5480 hardening

- Disabled light httpd port 5480 on Collector. Collectors need to be registered by running this script: `phProvisionCollector --add <user> <password> <super IP or host>`

```
        <organization> <collectorName>
```

Resolved issues

Id	Severity	Module	Summary
429644	Minor	GUI	User Activity Window does not properly show full name for users.
432791	Minor	GUI	Increase password length limit from 32 characters to 64 characters.
465797	Minor	Discovery	Test connectivity task for OKTA with large number of users may fail.
502929	Minor	App Server	Smart Scan discovery does not ignore devices already in the CMDB.
505759	Minor	GUI	Incidents are not triggering for failed STM.
507368	Minor	App Server	CMDB Rule Exception report shows exceptions from other Organizations.
511230	Minor	GUI	User full name is not displayed in the user traffic report.
517223	Minor	Agent	Windows Agent Installation error on Windows Server running PowerShell 5.1.
520294	Minor	Agent	Windows DNS parser with collection via Agent does not work if Detailed Debug DNS is NOT enabled.
521194	Minor	GUI	The Due Date in Create Ticket via Notification Policy should Be Relative Time.

Id	Severity	Module	Summary
517223	Minor	Agent	Windows Agent Installation error on Windows Server running PowerShell 5.1.
520294	Minor	Agent	Windows DNS parser with collection via Agent does not work if Detailed Debug DNS is NOT enabled.
521194	Minor	GUI	The Due Date in Create Ticket via Notification Policy should Be Relative Time.
522672	Minor	App Server	Exporting PDF reports fails after host upgrade from 5.0.0.
522810	Minor	System	CURL problems resulting undefined behavior including deadlock.
522824	Minor	App Server	Scheduled Reports runs twice on Execution.
522857	Minor	App Server	The deviceInfo/PerfMonitor REST API may take long time to load.
523287	Minor	App Server	HTML Role Management may take a long time to load.
523654	Minor	App Server	Large Active Directory discovery may be slow.
524273	Minor	App Server	String Longitude value in Identity Location Identity XML causes invalid XML
525052	Minor	Data Manager	Excessive "event without host attribute" error logs for summary dashboard.
525333	Minor	App Server	Last Login Date conversion in CMDB Report is not correct.
526306	Minor	App Server	CMDB Report loading can be slow when CMDB is large.
528698	Minor	Data Purger	Log integrity signature update to PostGress DB can be slow.
529008	Minor	App Server	CMDB Device delete can be slow when CMDB is very large.

Id	Severity	Module	Summary
529205	Minor	GUI	CSV Report export has data in exponential format.
529795	Minor	App Server	Scheduled report may run as inline report and not get data.
530642	Minor	Parser	Collector EPS may be a large number when event dropping rules are in action.
531851	Minor	App Server	CSV Export event shows receive time and device time to be 1 hour ahead of current time.
532784	Minor	Query Engine	Excessive PH_REPORT_VALUE_TYPE_ UNSUPPORTED errors reported by phReportMaster.
532800	Minor	GUI	HTML Role definition shows Flash GUI elements.
533985	Minor	Performance Monitoring	Fortinet QoS statistics for bytes and packet drops not being pulled.
534857	Enhancement	Parser	Vulnerability upload from Parser to AppSvr contains unnecessary information, causes processing delay on App Server.
535344	Minor	Performance Monitoring	Fortinet Link usage dashboard does not show Jitter/Latency/Pkt Loss.
535926	Minor	Performance Monitoring	Monitor inbound and outbound QoS for FortiGate Interface Usage Monitoring.
500588	Enhancement	App Server	Allow users to configure multiple SNMP Trap / SMTP servers for notifications.
510555	Enhancement	GUI	Enhance the time axis in Bar trend and line trend chart based on length of time window.
519377	Enhancement	System	Add flexibility for FortiSIEM to have better event database compression (at low EPS).
519870	Enhancement	System	Need to enable HTTPS and PowerShell for Windows Remediation (WinRM protocol).

Id	Severity	Module	Summary
534857	Enhancement	Parser	Vulnerability upload from Parser to App Server contains unnecessary information, causes processing delay on App Server.

Common Vulnerabilities and Exposures

Bug ID	CVE references
529300	FortiSIEM 5.2.1 is no longer vulnerable to the following. CVE Reference: • CVE-2018-13378