FortiSIEM - Release Notes

Version 5.3.3

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 5.3.3 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 5.3.3 Release.

What's New in 5.3.3

This document describes pre-upgrade instructions, new features, bug fixes, and enhancements for the FortiSIEM 5.3.3 release.

New Features

This release includes the following new features:

Use Pre-Computed Results in Search

Aggregated Searches with large time windows can be very expensive, specially in a high EPS environment. This release enables you to set up pre-computation schedules and then run searches against pre-computed results. Since FortiSIEM obtains the final search result from pre-computed results, searches can finish quickly.

See Searches Using Pre-Computed Results.

Enhancements

This release adds the following enhancements to FortiSIEM:

Linux Agent for SUSE Linux and Ubuntu 20

This release adds Linux Agent support for these systems:

- SUSE Linux Enterprise Server (SLES) – version 12 and 15
- Ubuntu 20

A few minor changes are required during installation – see Installing Linux Agent for details.

Elastic Cloud as Event Database

This release adds support for Elastic Cloud for FortiSIEM installations in public clouds.

See Elastic Cloud using REST API for details.

AlienVault OTX Integration for External Threat Integration

This release enables you to download Malware IP, URL, Domain, and Hash from the AlienVault OTX service.

See Working with AlienVault OTX for details.

Bug Fixes and Enhancements

This release includes the following bug fixes and enhancements:

ID	Severity	Module	Summary
644410	Minor	App Server	Widget Dashboard Imported in Super Global is not shared in organizations.
644090	Minor	App Server	Custom Event Attribute names do not display in CSV reports.
643967	Minor	App Server	Handle the Null pointer exception in App Server to Query Master communication.
643648	Minor	App Server	Query time interval is not saved properly in Report Bundle scheduled for organizations.
643249	Minor	App Server	An exception occurs during app server start up while loading namedValue to Redis.
640569	Minor	App Server	After upgrade, Shared dashboards created in Super Global are invisible if su to organizations.
637264	Minor	App Server	Failed to save location for device when city/state has a single quote (after it already triggered an incident).
635420	Minor	App Server	Device hostnames containing a single quote cause incident insert errors.
527733	Minor	App Server	LDAP user discovery merge is logging excessive user contact update.
497314	Minor	App Server	LDAP OU discovery is aborted because of long OU name.
647601	Minor	Data	"System License Warning: Max Number of Devices Exceeded License" rule does not trigger.
644155	Minor	Data	Some attributes are not correctly parsed by NetBotzCMCTrap.
641317	Minor	Event Pulling	Logon Events are not pulling from Google App Suite.

ID	Severity	Module	Summary
649152	Minor	GUI	Home Setting does not show on UI after an upgrade.
648413	Minor	GUI	winexe is enabled in Discovery once you edit a Discovery template.
647769	Minor	GUI	You can select any attribute in a rule exception. It should only allow those attributes in "Incident attribute".
644073	Minor	GUI	New schedule for FortiGuard IOC Service does not show the created schedule after saving.
643888	Minor	GUI	Losing the connection to Super during a Dashboard slideshow causes a user log out after 10 minutes.
640894	Minor	GUI	Pull Events tab shows an error from another organization.
638148	Minor	GUI	The GUI displays 0xA0 characters in Raw events as 0x20.
633235	Minor	GUI	GUI Error occurs when saving Access Method configuration for FortiGate Rest API.
632413	Minor	GUI	During GUI login, DOMAIN is not displayed until the Log On button is pressed.
612331	Minor	GUI	Dashboard Slideshow times out after 1 day.
611930	Minor	GUI	Generating two reports that attempt to show average and max value only shows max.
602326	Minor	GUI	CMDB Reports with Report Type generate a PSQLException.
598485	Minor	GUI	Parser Validation cannot handle parsers with an "&" symbol.
639744	Minor	GUI, App Server	Login drop down has to convert to text box in order to protect end client from exposure of other domains.
637664	Minor	H5_Analytics	In Rule Exception, the Value field cannot be edited when values are added from the CMDB.
596560	Minor	Parser	The character "<" in the test event breaks attributes display in Parser testing
629489	Minor	Performance Monitoring	Cisco ASA memory utilization polling fails as vendor has changed SNMP OID.
517105	Minor	Performance Monitoring	Memory utilization on Cisco Nexus 9k is stuck at 100%.
637631	Minor	Query Master	CSV Export from the date before daylight saving change shows a one hour difference.
648971	Minor	System	phDataPurger crashes when archiving from Elasticsearch to NFS if the raw event size is more than 64KB.
643027	Minor	System	FSM collector nodes contain passwords in plain text based on the API cache.
632883	Minor	System	Elastic Search Disaster Recovery does not sync the Redis

ID	Severity	Module	Summary
			Password correctly.
630634	Minor	System	Elasticsearch snapshot creation fails during disaster recovery.
644882	Enhancement	App Server	Support device names with single quote.
632976	Enhancement	App Server	Malware IP download - does not handle CIDR notation.
644104	Enhancement	Data	Need additional JunOS event types to the data-definition file.
643874	Enhancement	Data	Watchguard Firewall Parser needs an update.
643780	Enhancement	Data	Trend Micro Apex Central Parser for Antivirus doesn't create a correct Event Type.
643015	Enhancement	Data	Sophos Event parser does set the reporting IP or host name.
639125	Enhancement	Data	Windows WMI events in French are not fully parsed.
637703	Enhancement	Data	Citrix Netscaler Parser does not parse certain VPN logs.
632767	Enhancement	Data	Spanish Windows parser needs more translations.
615340	Enhancement	Data	Citrix Netscaler Parser does not parse out Group Names with a space.
612914	Enhancement	Data	Infoblox parser - Parser does not pick up client hostname in the syslog field. Instead, it picks up the IP address.
609725	Enhancement	Data	Windows Custom Log Parser does not parse out two fields for event ID 411: Client IP and Error Message.
603557	Enhancement	Data	Nessus Parser Host Field must also parse the hostname.
599955	Enhancement	Data	Windows Event Parsing - Language translation update.
643287	Enhancement	GUI	Domain part of O365 Endpoints need to be configurable.
641357	Enhancement	GUI	Country Groups must be editable only from the left tree.
640064	Enhancement	GUI	Cannot clear multiple incidents under the Incident Explorer dashboard.
612285	Enhancement	Parser	O365 Event Type MS_OFFICE365_SecurityComplianceCenter_AlertTriggered is missing details.

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`"

STIX/OTX Malware IOC Integration Error

If you see the error below when you log in to Glassfish, it is likely caused by the `jsse.enableSNIExtension` flag that was added to resolve a `httpd` issue in Java JDK 7. In JDK8, there is no need to set this flag.

Error:

```
#|2020-09-
10T12:30:00.535+0200|SEVERE|glassfish3.1.2|com.accelops.service.threatfeed.BaseOTXUpdat
eService|_ThreadID=218;_ThreadName=Thread-
2;|org.springframework.web.client.ResourceAccessException: I/O error on GET request for
"https://otx.alienvault.com/api/v1/pulses/subscribed?limit=20&modified_since=2020-09-
03T12:30:00%2B02:00&":Unsupported record version Unknown-0.0; nested exception is
javax.net.ssl.SSLException: Unsupported record version Unknown-0.0
```

To resolve this issue, follow these steps:

1. Log in to the Supervisor node.
2. Run the command `su - admin`.
3. Enter your Glassfish password and run this command `/opt/glassfish/bin/asadmin delete-jvm-options -Djsse.enableSNIExtension=false`
4. Run the command `Killall -9 java`.