FortiSIEM - Release Notes

Version 5.3.1

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 5.3.1 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
05/29/2020	Initial version of FortiSIEM 5.3.1 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 5.3.1 Release.

What's New in 5.3.1

This document describes pre-upgrade instructions, bug fixes, enhancements, and known issues for the FortiSIEM 5.3.1 release.

Pre-upgrade Notes

If you are upgrading from FortiSIEM release 5.2.x or earlier to 5.3.1, then read the FortiSIEM 5.3.0 Pre-upgrade Notes.

Bug Fixes and Enhancements

This release includes the following bug fixes and enhancements:

ID	Severity	Module	Description
631433	Major	Upgrade	App Server has an exception that caused the Redis cache to be incompletely populated during App Server start up.
633552	Major	Upgrade	5.3.0 upgrade fails often, resulting in inconsistent database passwords.
633142	Major	Upgrade	phRuleMaster and phIpIdentityWorker are down after upgrading the Super to 5.3.0.1658.
603845	Major	App Server	Risk score calculation storage saves excessive disk space in PostGreSQL
636430	Minor	App Server	Number of user sessions grow if REST API is invoked frequently.
636933	Minor	App Server	Excessive emails are sent out when a Ticket escalation policy is violated.
634518	Minor	App Server	The Cleared/Resolved incident count is incremented instead of creating new incidents.
628730	Minor	App Server	The Supervisor is using too many connections for the ServiceNow device integration.
629681	Minor	App Server	After an upgrade to 5.0, the user is unable to login if two users have the same user name in the same organization.
627395	Minor	App Server	A PH_DEV_MON_PERFMON_DEVICE_DELAY_HIGH event is generated unnecessarily because of disabled monitors.

ID	Severity	Module	Description
632282	Minor	App Server	FortiSIEM User accounts could not be locked again once they were unlocked.
633120	Minor	App Server	The Super/Global Identity and Location / Summary dashboards do not work if they have different display columns.
630561	Minor	App Server	The Incident Search by Id fails when a Rule is deleted.
572484	Minor	Data	Differences between the Country Names in GUI and the Geo Database cause rules/reports using country names to fail to trigger. The workaround is to use the Country Code instead of the Country Name. This release fixes the issue.
632838	Minor	Data	Windows Agent logs for French OS are not parsed correctly because of an extra space in French keywords.
459789	Minor	Data	Cannot parse one of the log segments for the Imperva device.
628778	Minor	Discovery	The firmware version of the FortiGate hardware devices are not polled correctly beginning with FortiGate version 6.0.5.
612331	Minor	GUI	Dashboard slideshow times out after 1 day.
611534	Minor	GUI	Cases display an Overdue state when they were closed before the due date.
630762	Minor	GUI	Enhanced Widgets for the Interface Usage Dashboard for Netflow and QoS.
632925	Minor	GUI	The Attack dashboard and the Incident > List > Category do not display when there is a rule with a missing Category or Subcategory.
633037	Minor	GUI	The Admin password change does not work for a first time login from the Storage setup page.
613018	Minor	Parser	Failed DNS lookups may cause a Collector to drop logs in high EPS scenarios.
629988	Minor	Parser	DNS name resolution does not work for Netflow events.
629517	Minor	Parser	Clear the Checkpoint certificates and configurations cached by backend.
635027	Minor	Query	The NFS Online Query is slow when Archive is also defined. It also has slower disks compared to Online.
631496	Enhancement	Data	Added a parser for the Broadcom SSLv Load-Balancer.
633775	Enhancement	Data	Enhanced Windows security log parsing for ID 4624, because logs differed between Windows Server 2012 and 2016.
629479	Enhancement	Data	The event type SophosXG-Event-SSLVPNAuthentication-Authentication needs additions for success and failure.
622987	Enhancement	Data	The Palo Alto Network Firewall configuration pull displays differences that were caused by dynamic certificates in the configuration.

ID	Severity	Module	Description
63173	Enhancement	Data	Parse more fields in the Checkpoint CEF log.
628104	Enhancement	Data	Error message "PHBoxparser Failed to execute node: collectAndSetAttrBySymbol".
627760	Enhancement	Data	The Palo Alto Firewall has more logs that are not parsed.
629261	Enhancement	Data	Improvement to the Azure Event Hub Parser.
635481	Enhancement	Parser	FortiSIEM does not set Owning Organizations for IP during Geo table lookups.

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`"