FortiSIEM - Release Notes

Version 5.2.7

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 5.2.7 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
01/11/2020	Initial version of FortiSIEM 5.2.7 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 5.2.7 Release.

What's New in 5.2.7

Bug Fixes

This release fixes the following vulnerability.

FortiSIEM installations have a hardcoded SSH key for a specific user (name: tunneluser) that allows anyone to authenticate as tunneluser to the Supervisor over SSH ports 22 and 19999.

Upgrade Notes

1. This release ONLY provides an upgrade for all platforms.
2. If you want to install FortiSIEM 5.2.7, then follow these steps
   a. Install 5.2.6 or earlier.
   b. Choose the final event database storage: local disk, FortiSIEM EventDB on NFS or Elasticsearch.
   c. Then upgrade to 5.2.7.

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`"