



# Release Notes

VSP Patch Version 2.3.5

[www.virsec.com](http://www.virsec.com)  
[support@virsec.com](mailto:support@virsec.com)



## Contents

1. Version.....	3
2. Date of Release .....	3
3. Fixes.....	3
4. Known Issues .....	3
5. Contact Information .....	4

Virsec Security Platform (VSP) leverages the patented Trusted Execution™ technology to protect high-value enterprise applications deployed in data center or on public and hybrid clouds, from highly sophisticated attacks including memory corruption, code injection, credential theft, supply chain and other sophisticated attacks. VSP effectively creates and enforces guardrails around the application as it executes. These guardrails ensure that applications only perform as intended and restrain bad actors from corrupting memory as a precursor to hijacking control of the application and subsequent stealing or destroying high-value enterprise data.

## 1. Version

Patch 2.3.5

## 2. Date of Release

5/10/2022

## 3. Fixes

Defect ID	Description
HMM-1713	cmd.exe is reported to CMS for past events too
HMM-1903	Stop Maintenance does not behave as expected if the probe is in Pristine Host mode
PLT-812	Hide vsp-cli start/stop options in the help menu
V2-13019	Unable to restart VSP services when /var file system is at 100%
V2-22342	Host Monitoring - HOST Scan error encountered after creating Host Profile for Probe
V2-22354	Mongo pod displays to CrashLoopBackOff error
V2-22357	Multiple incidents of type "Child process application policy violation" are reported within a minute
V2-22358	Java application crashes due to memory leak
V2-22398	Email server generates emails every minute

V2-22463	CMS internal server error (503 error) is displayed on File Events page
V2-22470	Probe erases Satellite software on installation
V2-22477	Error is displayed while trying to login to VM CMS (500 error) with cms-client service status unhealthy
SUPP-147	Exception Logging Time Stamp is incorrect. Impacts timeframe viewer in UI
SUPP-159	Dockerized CICD tool is not working

Table 1 – VSP 2.3.5 Fixes

## 4. Known Issues

Category	Description	Known Issue/ Caveat
<b>Host Monitoring</b>		
<b>Windows library issue</b>	In Windows, VSP host monitoring does not suspend already running processes that have non-whitelisted libraries loaded into it	<b>Known Issue</b>
<b>Linux HMM agent limitation</b>	In Linux, VSP host monitoring injects its own HMM agent into every running process. The HMM agent expects a specific version of <code>glibc</code> . If the application loads its own custom <code>glibc</code> version that is not compatible with the HMM agent, the HMM agent may not load correctly causing some application issues	<b>Limitation</b>
<b>Windows application execution inconsistency</b>	In Windows, an application can be started with or without its <code>.exe</code> extension. Since VSP host monitoring analyzes the commandline as is, running <code>python.exe</code> vs <code>python</code> may result in different detections	<b>Limitation</b>

Table 2 – Known Issues

## 5. Contact Information

In case of any questions, please contact Virsec Systems at [1-877-213-3558](tel:1-877-213-3558) OR [support@virsec.com](mailto:support@virsec.com).

-- END OF DOCUMENT --