



Release Notes

VSP Patch Version 2.4.2

www.virsec.com
support@virsec.com



Contents

1. Version.....	3
2. Date of Release	3
3. Fixes	3
4. Known Issues	4
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 2.4.2

2. Date of Release

5/18/2022

3. Fixes

Defect ID	Description
WEB-1660	Java application crashes due to memory leak
HMM-1968	Stop Maintenance does not behave as expected if the probe is in Pristine Host mode
CMS-3494	CMS installation script displays “ Error response from daemon: no such id ”
CMS-3545	Error 403 is encountered while connecting to Zendesk account
CMS-3579	Kubernetes probe is not provisioned
SUPP-167	Dashboard Top N Hosts stopped working as of 2.2.0
SUPP-174	Cannot use FIM File Extension Exclusion list to exclude noisy hidden linux files

Table 1 – VSP 2.4.2 Fixes

4. Known Issues

Category	Description	Known Issue/ Caveat
Host Monitoring		
Windows library issue	In Windows, VSP host monitoring does not suspend already running processes that have non-whitelisted libraries loaded into it	Known Issue
Linux HMM agent limitation	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	Limitation
Windows application execution inconsistency	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	Limitation

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.

-- END OF DOCUMENT --