Release Notes

VSP Patch Version 2.3.3

www.virsec.com
support@virsec.com

Contents

Virsec **S**ecurity **P**latform (**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 2.3.3

2. Date of Release

3/28/2022

3. Fixes

Defect ID	Description
V2-22201	log4j Java Class files removed from Kafka and Zookeeper
V2-22217	Custom certificate is not applied in AWS EKS
V2-22237	HMM Incidents are throttled so that CMS is not flooded with many incidents
V2-22249	Windows Default ACP Rule matches incorrect process name `net.exe`
PROD-54	rootCA Support in CMS for custom SSL certificates
SUPP-106	Probes are disconnected after a CMS restart. Probes have to be restarted to move to Connected state

Table 1 – VSP 2.3.3 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 `glibc`. If the application loads its own custom `glibc` 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 `.exe` extension. Since VSP host monitoring analyzes the commandline as is, running `python.exe` vs `python` 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 OR support@virsec.com.

-- END OF DOCUMENT --