Release Notes

VSP Patch Version 2.4.1

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 2.4.1

2. Date of Release

4/19/2022

3. New Feature

1. **HMM Incident Throttling –** VSP-Host now has a throttling mechanism to prevent flooding of incidents to CMS. The throttling works at two levels:
   a. **Generic incidents** have a maximum number of incidents for a time interval
   b. **ACPs** have a separate mechanism that limit the number of incidents per application and per ACP

4. Fixes

Defect ID	Description
HMM-1713	Incident tickets event time matches the offending process starting timestamp and not when the incident was recorded by HMM
HMM-1721	In previous releases, the child process ACP incidents are not throttled
HMM-1745	FSM provisioning fails in all Hosts with Sidecar configuration
HMM-1979	HMM process fails in probes (both containers and VMs) due to a shared memory key overlap

SUPP-21	VSP user invitation link takes user to incorrect address
SUPP-140	Probe Installer Fails on Windows 2019 with the error `"Failed to Copy vsp_probe.cfg file"`
SUPP-158	Web Profile Exception Rules are not downloaded to the Probes
PLT-812	Hide vsp-cli start/stop options in the help menu

Table 1 – VSP 2.4.1 Fixes

5. 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

6. Contact Information

In case of any questions, please contact Virsec Systems at 1-877-213-3558 OR support@virsec.com.

-- END OF DOCUMENT --