Release Notes

Virsec Security Platform 2.4

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 centers or on public and hybrid clouds, from highly sophisticated attacks including memory corruption, code injection, credential theft, supply chain and others. 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

2.4.0

2. Date of Release

3/14/2022

3. Compatibility Matrix

Refer to the Compatibility Matrix for information related to the Supported platforms and languages

4. New Features

1. **PHP 7.4 Support –** 2.4.0 adds VSP-Web support for PHP 7.4. Refer to the Compatibility Matrix for more information
2. **ALPINE 3.7 Support –** 2.4.0 adds VSP-Host and VSP-Memory support for ALPINE 3.7 on containers. Refer to the Compatibility Matrix for more information
3. **AppDynamics Compatibility Improvements –** VSP-Web runtime instrumentation can be deployed alongside AppDynamics APM instrumentation. The configuration is simplified to reduce the manual steps and enhance user experience
4. **VSP Probe as Service –** VSP Probe is now installed as a service on Linux systems
5. **Windows Recommended ACPs –** VSP CMS Windows ACPs have been enhanced to cover a large number of MITRE techniques
6. **LFR Feature Improvements –** LFR now has an option to turn off resync on container restart. The artifactory sync is now on a persistent volume and not a part of the container.

5. Known Issues and Caveats

Category	Description	Known Issue/ Caveat
Installation		
CI phase fails on Ubuntu 20 container	CI phase fails on Ubuntu 20 container if the docker version 19.03.0 - 19.03.8 is installed on the Management node used for installation. This is due to a known issue in these docker versions **Recommended Workaround:** Install docker version: 19.03.9 on the Management Node	**Known Issue**
After CMS upgrade, Probes status is wrongly depicted	After CMS upgrade, Probes page depicts the wrong AI status, even though keep alive messages are not received from ASI **Recommended Workaround:** Copy/Mount redisvolume directory to worker nodes after CMS restart/upgrade	**Known Issue**
CI phase installation fails for “In App” Mode of deployment	CI phase installation fails for “In App” Mode of deployment in cases where jdk is already installed on the base container image **Recommended Workaround:** Utilize sidecar mode of deployment	**Known Issue**
FSM (File System Monitoring)		
File Rename incident is detected with "fileName" and "filePath" as "NON_MONITORED_PATH"	For a File rename incident, "fileName" and "filePath" attributes are reported as "NON_MONITORED_PATH" after deleting the contents of the file	**Known Issue**
Modification of Hard-link files are not reported as incidents	Modification of Hard-link file is not reported as incidents	**Known Issue**
Modification of Soft-link files are not reported as incidents	Modification of Soft-link files are not reported as incidents	**Known Issue**

VSP-Memory		
Post BE attack, process may not restart for VM	Post BE attack, if an application is configured in the inline protect restart mode, it may not get restarted successfully. **Recommended Workaround:** sudo must be present on the machine and must not require a password to execute when launched as root user	**Known Issue**
Apache 2.4 (httpd) is not instrumented when it is started as a service (Win 2016)	httpd service is not instrumented when it is started as a service. The process terminates. **Recommended Workaround:** Do not start httpd as a service. Execute it from the console	**Known Issue**
(Windows) VSP-Memory fails to automatically re-instrument an Application sometimes	In Windows, when using auto-instrumentation for a service, VSP-Memory sometimes fails to re-instrument the application automatically, if the service is restarted via the Services window. This is because VSP-Memory-Assist does not process the application stop/start quickly enough **Recommended Workaround:** In such cases, stop the service, wait up to 5 seconds before starting the service	**Known Issue**
Host Monitoring		
All entries in the Global exclusion list are considered regular expression patterns	All entries in the Global exclusion list are considered regular expression patterns even if there are absolute paths present	**Known Issue**
SearchUI.exe process gets suspended on Windows Server 2016	SearchUI.exe process gets suspended on Windows Server 2016. This is a behavior of the specific OS	**Caveat**
VSP-CLI logs error in Mixed Mode	In Mixed Mode, VSP-CLI logs error: "`ERROR: ld.so: object 'libvsp-hmm-agent.so' from /etc/ld.so.preload cannot be preloaded: ignored.`" It has no adverse effect on the VSP-CLI functionality.	**Caveat**
Some publishers did not get detected/whitelisted during initial scan	Upon launch, Google Chrome browser, some libraries (signed by publisher '`ESET, spol. s r.o.`') are loaded. The publisher is not listed in the publishers list in the initial scan. When the process is launched, this publisher gets whitelisted automatically (if auto-whitelist is enabled)	**Expected Behavior**

Suspended signed process is not resumed (Windows)	After the initial scan, when a new process is installed, it gets suspended in Protect Mode. When the publisher is whitelisted, the process is not resumed. **Recommended Workaround:** Whitelist the specific process associated with the profile.	**Known Issue**
VSP does not report modified processes or libraries that belong to a package in systems that use prelink	VSP does not report modified processes or libraries that belong to a package in systems that use prelink. The prelink application inherently changes the binary checksum, so there is no true reference for VSP to use.	**Expected Behavior**
In Windows, when an application is started with or without the ".exe", different detections by VSP may be possible	ACPs are specific to the command line used when starting an application. In Windows, when an application is started with or without the `".exe",` different detections by VSP may be possible	**Known Issue**
App Control Policies do not support any unicode character in any field	App Control Policies do not support any `unicode` character in any field	**Limitation**
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**
Execution of native image DLLs by Windows CLR runtime is not covered	Execution of native image DLLs by Windows CLR runtime is not covered under Virsec Process and Library Monitoring capabilities	**Known Issue**

Reporting		
On premise deployment: Generated Reports cannot be viewed	In an on-premise multi-pod deployment, generated reports cannot be viewed. Error 404 is displayed. This occurs when the components JReports and Ngnix Client service are deployed on different worker nodes	**Known Issue**
VSP-Web (on Web Server)		
Compressed Responses are not supported	VSP-Web (on Web Server) does not support compressed Responses. Example: `gzip`	**Limitation**
VSP-Web		
Long polling or WebSocket based requests are not supported	Long polling or WebSocket based requests are currently not supported by VSP-Web	**Limitation**
Asynchronous servlet model is not supported	Applications leveraging Async-API are not supported	**Limitation**
Permission denied message is displayed along with the Application message	For some inline protection cases, along with the Permission Denied pop-up message, the application response is also displayed	**Known Issue**
VSP Memory Exploit Protection		
Process Hollowing prevention does not work under some conditions	Process Hollowing prevention does not work under some conditions due to the way API hooking is implemented	**Known Issue**
RMP does not detect a variant of PowerShell Exploit	RMP does not detect a variant of PowerShell Exploit if both the source and target processes are the same	**Limitation**
RHEL 7.6: Process name in Memory integrity incidents is inaccurate	Process name in Memory integrity incidents is displayed as bash instead of the target process name	**Known Issue**

General		
VSP-CLI command gives error while executing stop/restart VSP-Manager service	When VSP-CLI command is used to stop/restart VSP-Manager service (individually or all the services), there is an error “Exception occurred during the initialization of the VSP Kafka consumer” **Recommended Workaround:** Close the current session and stop/restart the VSP-Manager service in a new session	**Known Issue**
User may be unable to delete instances	User may be unable to delete instances in a larger environment with more than 20 thousand open incidents	**Known Issue**
Application and host profiles do not auto- associate if the tag names contain spaces	Application and host profiles do not auto- associate if the application and host tag names contain spaces **Recommended Workaround:** Ensure that no spaces are present in the tags	**Limitation**

Table 1 – Known Issues and Caveats

6. Contact Information

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

-- END OF DOCUMENT --