Release Notes

VSP Patch Version 2.4.4

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 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 2.4.4

2. Date of Release

7/18/2022

3. New Features

1. By default, VSP Memory Exploit Protection now terminates the source and target processes in Protect Mode
2. The parameter defining the ASI IP (-i) is now made optional for Probe installation on Linux and Windows VMs
3. VSP-Host now supports the Operating System: SUSE 12. Refer to the Compatibility Matrix for more information

4. Fixes

Defect ID	Description
SUPP-375	Unable create new rule for an existing ACP
SUPP-374	Unable to edit ACP command-line rules
SUPP-324	Webhook sends file integrity alerts even when they are not configured
SUPP-309	Legitimate process is BLOCKED after switching to Protect Mode

SUPP-308	ACP does not block the command line in protect mode during certain attempts
SUPP-306	Unable to switch custom MS Exchange build to Protect mode
SUPP-305	User ACP rules generate incorrect incidents
SUPP-302	Web provisioning fails on containers
SUPP-297	Need better error handling for VSP CI
SUPP-294	Partial Probes get exported from CMS console probe page when all probes are selected during export
SUPP-291	Nginx fails to start due to the VSP-Memory copying the wrapper over binary
SUPP-289	Connection Error occurs while attempting to save an updated ACP rule
SUPP-288	Windows Strict v2.0 ACP generates false positives in hosted POV environments
SUPP-287	User is unable to log in to .NET (32bit) based Application after instrumentation
SUPP-285	Syslog Custom Extension Keys are not compliant with CEF Standard
SUPP-282	Documentation: Sophos instructions missing exclusion entry information
SUPP-279	RXSS for internal IPs and False positive SQLi incidents reported
SUPP-278	Probes do not auto connect to CMS after VSP upgrade
SUPP-250	FSM agent fails to create file event and report it to CMS (except file removed event)
SUPP-174	Cannot use FIM File Extension Exclusion list to exclude noisy hidden linux files
HMM-2936	Explorer.exe from Windows folder gets suspended by Strict ACP
CMS-4815	Update Installation Checklist with revised CMS RAM settings for VM install
CMS-4811	Out of Sync Hosts - Mouseover Text has Spelling Mistake
CMS-4762	LDAP User authentication fails when BindDN user account (used for LDAP auth) is in a user directory that is different from BaseDN
CMS-4288	LDAP user is unable to access CMS console if the default role is set to none

Table 1 – VSP 2.4.4 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 --