Release Notes

Virsec Security Platform 2.5

www.virsec.com
support@virsec.com

Contents

1. Version 3
2. Date of Release 3
3. Compatibility Matrix 3
4. New Features 3
5. Fixes 5
6. Known Issues and Caveats 7
7. Contact Information 13

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

2.5.0

2. Date of Release

9/12/2022

3. Compatibility Matrix

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

4. New Features

1. **Platform and CMS Enhancements:**
    a. **CMS UI** has improvements to ease the Application creation process:
        i. Fields removed: Application Context Path, Inline Protection Mode
        ii. Fields Made Optional – Process Description
        iii. Protection Mode can now be defined at a vulnerability level
    b. Terminology Change – “Whitelist” and “Blacklist” are replaced with “AllowList” and “DenyList“
    c. **rootCA Certificates:** CMS now supports rootCA certificates
    d. **Proxy Server NTLM Support:** Existing Proxy Server configuration is enhanced to support NTLM Authentication
    e. **VSP License Restructuring:** VSP licenses are modified to match the pricing changes
    f. **Secure Kafka Channel:** User can now select unsecure, one-way SSL or two-way SSL secure channels

g. **Interoperability testing:** VSP is tested to function with third party anti-virus products like Sophos, Trend Micro, McAfee, Symantec, Comodo. Refer the troubleshooting documentation for more information

2. **Compatibility Enhancements:**
   a. **RHEL 8 CMS Deployment:** Support for CMS deployment on RHEL 8 is added
   b. **VSP-Host:** Support for RHEL and CentOS 6.10 32 bit VM is added
   c. **FSM:** Windows 2008 R2 64-bit, RHEL/Centos 6.5 and 6.7 support is added for FSM
   d. **VSP-Web: Java 17 Support:** Support for Java 17 is added. Refer to the Compatibility Matrix for more information
3. **VSP-Web**
   a. **Web Adaptive Instrumentation:** The In-App WAF (Adaptive Instrumentation) tries to mitigate compatibility issues by downgrading attack detection to HTTP req/res message only if instrumentation is not possible for all system events
   b. From 2.5.0, Web Profiles can be configured for App services which include rules related to protocol enforcement, rate limits and allow/deny
4. **VSP-Host**
   a. **Mounted Folders Auto-Exclusion:** In both Windows and Linux, the mounted folders are auto-excluded during the initial system scan
   b. **Linux Recommended ACPs** – VSP CMS Linux ACPs have been enhanced to cover a large number of MITRE techniques
   c. Latest ACPs recommended by Virsec are now available on the Artifactory
   d. Pristine Mode configuration is now available during Maintenance Mode also
   e. From VSP 2.5.0, by default, all the signed scripts are trusted similar to the processes and libraries
   f. Allowlists are downloaded faster on probes
5. **VSP Memory Exploit Protection**
   a. VSP provides coverage against the below exploits: (Refer the Operations Manual for the full coverage list)
      i. ***Windows:*** Thread Local Storage (Reported as Process Hollowing Incident), Thread Execution Hijack, Credential API Hooking
      ii. ***Linux:*** DirtyPipe
   b. **Enhanced Protection:**
      i. ***Windows:*** Effective from this release, the target process is also killed along with the source process (existing functionality)
      ii. ***Linux:*** Protection Mode is now supported

5. Fixes

Defect ID	Description
SUPP-431	Docs: Update public Gitlab docs until future container strategy is released
SUPP-405	Application functionality is affected after deploying VSP
SUPP-399	VSP-manager does not handle steady-state keep alive exceptions correctly
SUPP-395	Non binaries are reported from the initial FSWalk
SUPP-369	Incorrect reference to an ACP is applied to the Host Profile if the ACP name is similar
SUPP-366	Archived nodes cannot be deleted on CMS
SUPP-362	CMS is not resilient to server reboot in EKS
SUPP-361	Probes unable to reconnect to CMS console after CMS server reboot. CMS client reports 502 error
SUPP-357	Non-admin user cannot view alerts, threat and incidents on CMS dashboard
SUPP-355	Reflected XSS is not blocked for bookstore application
SUPP-354	Email notifications are not sent from CMS
SUPP-348	Failure to start CMS after execution of setup.sh during VSP upgrade from 2.4.0 to 2.5.0
SUPP-345	Application version number appears twice in the “Application” column
SUPP-344	In a Nginx Buffer Error Incident, the Memory Addresses are inaccurate
SUPP-335	VSP Upgrade on EKS from 2.2.4 to 2.5.0 fails
SUPP-333	License activation after upgrade to VSP 2.5.0 does not unlock CMS UI
SUPP-330	Azure SAML integration to be tested
SUPP-328	Log4j RFI attack is BLOCKED in protection mode but reported as a LOG incident in CMS
SUPP-327	App "File Integrity Exclusion Folders" field does not allow comma separated values
SUPP-273	IBM and IIS servers are not in PCM but feature in installation docs

SUPP-262	CMS UI Attack count is not updated
SUPP-250	FSM agent fails to create file event and report it to CMS for events except for file removed event
SUPP-216	Google found vulnerability in probe
SUPP-212	Infinite Potential | Host Out of Sync on Windows 2016
SUPP-208	ACP fails to detect useradd commands with `/dev/null` in it
SUPP-203	CI & CD tools are using images from internal artifactory
SUPP-201	Virsec 2.4.0 dashboard incident for Buffer Error displays 32-bit address for a 64-bit linux app
SUPP-200	High CPU Utilization on Probe on Windows 2016 server after upgrading probe from 2.2.2 to 2.3.3 while in Protect mode
SUPP-189	CI script encounters error with `-g` option
SUPP-186	Probe registration with CMS is not successful
SUPP-170	Connection error occurs while new scheduled reports are created in CMS
SUPP-155	Windows probe installer attempting to download `vsp-web-vm.zip` file from an incorrect location
SUPP-128	Unable to delete the previously associated but currently disconnected probe
SUPP-94	Probe installation takes a long time
SUPP-90	SKU script not able to detect the DD/MM/YY format
SUPP-73	VSP Probe install on RHEL takes 40 minutes when no Internet available
SUPP-66	Password reset does not work with all special characters
SUPP-52	False positive Web incidents reported
SUPP-46	CMS/LFR zip has UID of 1008. This value must be changed since it may be used by other UIDs
SUPP-43	'Activate now' link in the Email redirects to wrong URL after the user is invited by the super admin
SUPP-32	Windows probe installation frails
SUPP-9	Errors in CMS services: cms-client service and utility-service

Table 1 – VSP 2.5.0 Fixes

6. 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**
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 deletion of the file contents	**Known Issue**
Duplicate incidents and events are generated after file modification	Duplicate incidents and events are generated after modification of an existing or new file with event types NEW_FILE, FILE_MODIFIED and FILE_RENAMED	**Known Issue**
(Windows 2008) Two incidents are generated for file rename action	For a file rename action, two Incidents FILE_RENAME and FILE_MODIFIED are reported in Windows 2008	**Known Issue**
Incidents are reported for excluded folders	When multiple Applications are associated with the same ASI and a few folders are excluded in one of them and not the others, incidents are reported for the excluded folders **Recommended Action:** Ensure that the folders are excluded in all the associated Applications on CMS	**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/allowlisted 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 allowlisted automatically (if auto-allowlist 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 allowlisted, the process is not resumed. **Recommended Workaround:** Allowlist 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 lines 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**
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**
Exclusion on Child Type ACP rule does not work	Even when a child process added under exclusion in ACP, Child Exclusion is reported as incident	**Known Issue**
Incident is not reported when the user name is a mismatch	Incident is not reported when the user name does not match the "Allow" user in ACP config	**Known Issue**
Publisher/Package list is not included when the host profile is exported	Publisher/Package list is not included when the host profile is exported. As a result, when the host profile is imported into CMS, the publisher/packages list may be missing and may generate incidents.	**Limitation**
Fully statically-linked executables are not detected during the start up by HMM	Fully statically-linked executables are not detected during the start up by HMM. However, whenever the allowlist is published or there is a VSP host mode change, VSP host detects and checks the actively running statically-linked executables	**Known Issue**

For a small subset of applications started via the "service" command in Linux, VSP host does not detect the application start	In some cases, for a small subset of applications started via the "service" command in Linux, VSP host does not detect the application start, resulting in a potential false negative. However, each time the allowlist is published or the VSP host mode is changed, VSP host scans the system, that detects the running application if it is still running	**Known Issue**
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 Kubernetes - based deployment: Generated Reports cannot be viewed	In an on-premise Kubernetes - based 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**
Reports are not generated when the Report name contains a special character	Reports are not generated when the Report name contains a special character except "-" and "_"	**Known Issue**
The error, "Unable to connect to the Report Server" is displayed in CMS while scheduling a report	The error may be due to the occurrence of SQL connectivity error in the JReports Server. **Recommended Workaround:** If the error SQLNonTransientConnectionException is found, restart the JReports server	**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 2.5.0: VSP-Web for Ruby is not backward compatible	VSP-Web for Ruby on Rails is not backward compatible Impact: It impacts VSP-Web for Ruby, where CMS is upgraded to VSP 2.5 and Probe is still of a previous version Recommended Workaround: Ensure that VSP Probe is also upgraded to version 2.5	**Limitation**
RFI profile exclusion list is not considered for perimeter level RFI attack	RFI profile exclusion list is not considered for perimeter level RFI attack **Recommended Workaround:** Add the relevant exception to circumvent the issue	**Known Issue**
Web Protection (On Web Server)-Apache – pop-up is not displayed	Web Protection (On Web Server)-Apache: Permission denied popup is not displayed. The request is blocked as expected with no impact to functionality	**Known Issue**
.Net Core: VSP deletes comments from the file web.config	.Net Core: While provisioning application, VSP deletes comments from the file `web.config` of the application	**Known Issue**
Invalid CSRF token is reported to CMS when two j-session IDs are present	Invalid CSRF token is reported to CMS when two j-session IDs are sent in the request. VSP supports monolithic applications only. This occurs with multiple session providers only	**Known Issue**
VSP Memory Exploit Protection		
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 for watch command	Process name in Memory integrity incidents is displayed as bash instead of the target process name for watch command	**Known Issue**

Multiple incidents are reported for powershell	Multiple incidents are reported for powershell since Windows attempts to spawn a new powershell with a shortened path and VSP blocks all these attempts	**Expected Behavior**
Regex-based exclusions are not supported	Regex-based exclusions are not supported currently	**Limitation**
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**
For VSP CMS on an AWS environment ensure that only the External Email server is configured	For VSP CMS on an AWS environment ensure that only the External Email server is configured	**Limitation**
Email Subscription for application-based incidents	If any application-based incident is configured for Email Subscription, ensure that the Host is NOT selected	**Known Issue**
VSP is not supported for workloads running SELinux in Enforcing mode	VSP is not supported for workloads running SELinux in Enforcing mode	**Limitation**
CMS dashboard is not displayed for LDAP user with modified email ID	It is highly recommended to use email as the unique login attribute in the LDAP configuration. If CN is configured and the email ID is modified, CMS does not load the dashboard for that user	**Known Issue**
Emails configured with spaces in LDAP are not supported	Emails configured with spaces in LDAP are not supported. In such cases, a “valid object class error” is encountered on CMS LDAP configuration page for the section LDAP User Binding	**Known Issue**
Licenses need to be reloaded after an On-premise license server restart	Licenses loaded on the on-premise license server do not persist. Hence once the on prem license server is restarted with CMS restart they need to be reloaded/activated again using the activation id already shared	**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 2 – Known Issues and Caveats

7. Contact Information

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

-- END OF DOCUMENT --