Mandiant

PRODUCT UPDATE 4.9.0.0 - SEPTEMBER 22, 2022

MSV 4.10.2.2 contains defect resolutions and a critical security fix. We recommend you apply that update as soon as reasonably possible. If you're unable to upgrade at this time, use the instructions in **Manage User Admin Account** (https://docs.mandiant.com/home/manage-user-admin-account) to either set a password for the account or disable the account if it's not being used.

This note is for customers who meet the following criteria:

- Protected Theater is hosting images that use UEFI as the boot method
- Protected Theater is on a version earlier than 4.9.0.0/5.9.0.0 that needs to be updated

Before starting the upgrade, we strongly recommend that you take a snapshot of the PT VM first. Also, take note that that versions prior to 4.10.0.0 are EoSL as per **Security Validation Software Version Support** (https://docs.mandiant.com/home/msv-software-version-policy), so we also recommend that you upgrade to the latest available Security Validation release.

When UEFI is used as the boot method, Protected Theater versions before 4.9.0.0/5.9.0.0 were continually accumulating snapshots. As of 4.9.0.0/5.9.0.0, only a single snapshot layer is being maintained, with all prior snapshots being folded into that single disk layer. Before upgrading, check the available disk space on the volume storing the PT's images to determine if there's enough free space to successfully perform the upgrade.

To complete a PT upgrade to 4.9.0.0/5.9.0.0, or higher, from a version prior to 4.9.0.0/5.9.0.0:

1. Take a snapshot of the PT VM.
2. Check the number of snapshots & disk space required. To do this,
    a. Look in the **/opt/apps/verodin/node/images** directory & identify files that have a ten-digit number at the end of their filename. These are the snapshot layers that will get folded together into a single snapshot layer file on upgrade.
    b. Calculate the disk space required for the upgrade by adding up the file sizes of all the snapshot layers. Round up slightly to ensure a buffer of available disk space.
3. Add disk space, if necessary.
    a. If the sum total of all snapshot layers (from 1a) is greater than or close to the amount of free disk space remaining on the PT volume holding the images, increase the volume's disk space.
    b. If the sum total of all snapshot layers (from 1a) is less than the amount of free disk space, continue to the upgrade step.
4. Perform the PT upgrade.
5. Once the upgrade has completed, any disk space added to accomplish the upgrade can be reclaimed.

If you need any assistance with this process, please contact your TSC or CSM.

The Mandiant Security Validation (MSV) team is pleased to announce version 4.9.0.0 of the MSV platform.

General Enhancements

- GMail API now available as an option for Email Action notifications
- Enhancements to email-specific integration queries when searching for events upon completion of Action
- Failures to connect to proxy now show error result and are no longer blocked

Bug Fixes

- Fixed an issue with deleting a Protected Theater while connected to Protected Actor returning to Protected Theater screen
- Resolved Job Status Filter date/time not matching results
- Fixed VRegister failure to escape proxy password
- Resolved urllib3 errors when parsing proxy url
- Corrected http_ntlm not working with Windows Endpoint Actors
- Fixed issues in SEP Integration
- Fixed issue with Network Actors reporting inability to see Cloud Actor
- Fixed issue with backups persisting applied patches during Director restore
- Protected rule sets updated for Defender ATP
- Fixed Zscaler file download A100-362 failures due to 'non-RFC compliant traffic'
- Corrected issue with AEDA Configuration sleep time configuration
- Correctly resolve OOM Job Processor Errors
- Resolved 500 Internal Server Error issue under certain Director update scenarios
- Return expected Results when Scheduling repeating Bulk Evaluations
- Fixed issue with bulk scheduled repeating jobs not working
- Customer Report now correctly displays in older versions of MSV
- Update to MSV Linux Actor Standalone Installer Readme
- Fixed issue with Cybereason integration error handling
- Resolved issue with Host CLI commands not displaying correctly
- Corrected issue where certain job logs could contain plaintext data
- Director UI now correctly shows "Out of Disk Space" error message when a backup fails
- External snapshots for UEFI-boot PT guests no longer persist
- Corrected Drag and Drop Actions from Unassigned to Current in Queue
- MSV no longer sending the hostname of the source Actor as the login ID when using the http_kerberos proxy type
- Fixed Microsoft Sentinel integration alerts
- Resolved ZScaler proxy issues when using SAML auth
- Corrected AEDA Monitor Evaluation Job failure handling
- Scheduled Jobs no longer removed when canceled
- Large Bulk Jobs Fail to Execute on A Large Subset of Suitable Actors (But Run Fine if Ran individually)

Appliance OS Security Update

The Mandiant Advantage Security Validation Product team would like to announce the availability of a security update for the platform. This security update applies to Directors, Actors, and Protected Theaters that are virtual appliances. The criticality of the vulnerabilities resolved are listed below.

Mandiant uses **Red Hat's security ratings (https://access.redhat.com/security/updates/classification)** to determine the criticality of vulnerabilities identified and resolved. This rating system is a combination of a four-point scale and the Common Vulnerability Scoring System (CVSS) base scores. The criticality of the vulnerabilities resolved are listed below.

	Director	Actor	Protected Theater
Critical	0	0	0
High	1	1	0
Medium	0	0	0
Low	0	0	0

Details for the vulnerabilities against the Director are as follows:

- CentOS 7 : open-vm-tools (CESA-2022:6381)

Details for the vulnerabilities against the Actor are as follows:

- CentOS 7 : open-vm-tools (CESA-2022:6381)

You have two options for installing this security update:

> **Note**: Security updates should only be applied to appliances where automatic OS updates are not enabled (newly deployed agents as of 4.8.4.0 have automatic updates turned on by default).

- Via the Verodin GUI, using a Patch file (verodin_sec_update_4.9.0.0.patch). This requires you to be on version 4.9.0.0 or higher.
- Via the command line, using a tar.gz file (verodin_repo_4.9.0.0.tar.gz). This method allows you to apply the security patch to any version of the platform.

To download documentation and software (appliance images, installers, and update packages) visit the **Validation Section of the Docs Portal (https://docs.mandiant.com/home/security-validation-on-prem-and-saas)**.