Mandiant

PRODUCT UPDATE 4.9.2.0 - NOVEMBER 14, 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 4.9.2.0 of the MSV platform.

General Enhancements

- Added ability to assign a proxy to Webhooks
- HTTP GET file transfer actions now have a configurable timeout
- Email Theater Actions now report the SMTP ID of job sent emails
- Added MSI Integration Operational Status health checks
- As of November 15, 2022, a new support portal is available

Bug Fixes

- Fixed issue where endpoint events were not being collected appropriately
- Fixed issue where repeating actions were not inheriting the parent runtime parameters
- Fixed issue where the cleanup service would sometimes get locked in a stopped state
- Fixed issue that could cause Splunk notable event to only be tied to one action in an evaluation instead of all the relevant actions
- Fixed issue when restoring from a Director backup to prevent overwriting the known network configuration
- Fixed issue impacting detections for DNS queries
- Fixed issue with Host CLI commands disappearing
- Fixed issue where the Director Settings page would sometimes become out of sync
- Fixed issue in Report Builder to allow for 1-day or 2-day selections
- Fixed issue where the security update for actors was not properly displayed in the UI
- Additional minor bug fixes and improvements

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.

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	1	1	1
High	1	1	1
Medium	0	0	0
Low	0	0	1

Details for the vulnerabilities against the Director are as follows:

- CentOS 7: expat (CESA-2022:6834)
- CentOS 7: bind (CESA-2022:6765)

Details for the vulnerabilities against the Actor are as follows:

- CentOS 7: expat (CESA-2022:6834)
- CentOS 7: bind (CESA-2022:6765)

Details for the vulnerabilities against the Protected Theater are as follows:

- CentOS 7: expat (CESA-2022:6834)
- CentOS 7: bind (CESA-2022:6765)
- CentOS 7: java-1.8.0-openjdk (CESA-2022:7002)

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)**.