

PRODUCT UPDATE 4.12.1.0 - OCTOBER 26, 2023

The Mandiant Security Validation (MSV) team is pleased to announce version 4.12.1.0 of the MSV platform.



This update includes an upgrade to the internal Director database. Customers are strongly encouraged to **take a backup of the Director before upgrading** (<https://docs.mandiant.com/home/msv-backing-up-and-restoring-the-platform>).

General Enhancements

- Added support for **MITRE ATT&CK versions 13 and 13.1** (<https://attack.mitre.org/versions/v13/>)
- Updated Director PostgreSQL to version 13.12. This is to address PostgreSQL 11 becoming end of life as of November 9, 2023.
 - As part of the database upgrade, data is automatically migrated over to the new PostgreSQL 13 database. This process can take several hours depending on the amount of data.
 - Updating the database to PostgreSQL 13 requires duplicating the existing data for PostgreSQL 11.
 - If the free disk space is less than the space consumed by the DB, then you will have insufficient disk space for the upgrade. The upgrade will roll back and the status for it will read, "Verified, not yet applied." See [this troubleshooting document](https://docs.mandiant.com/home/msv-director-upgrade-failures) (<https://docs.mandiant.com/home/msv-director-upgrade-failures>) for more information.
 - To check the disk usage of the PostgreSQL DB by running the following command on the Director:

```
/bin/su - postgres -c "/usr/bin/du -s /var/lib/pgsql/11/data/"
```
 - To check the current free disk space on the Director run:

```
/bin/su - postgres -c "/usr/bin/df /var/lib/pgsql"
```
 - To address this issue, you'll either have to free up space or extend the volume using steps in this document: <https://docs.mandiant.com/home/msv-expanding-the-director-storage>.
 - Once successfully upgraded to 4.12.1.0, there will be a cleanup operation performed on a subsequent upgrade (4.12.2.0 forward) to reclaim disk space from the migrated database.
- Added support to add/modify the PassengerMaxRequests settings in httpd config. This can help in low memory situations.

Bug Fixes

- Fixed an issue where 4.12.0.0 Actors using a proxy configuration did not connect to the Director
- Fixed a logic bug where, in certain cases, Actors might become unresponsive before clearing all their running job status
- Increased the Director relay timeout to help reduce occurrences of Integration Actors timing out while processing large numbers of raw events
- Fixed an issue that prevented security technology detection and discovery for some jobs
- Fixed an issue where some successfully blocked actions were subsequently erroring out due to a missing mimikatz prompt
- Fixed an issue where Actor temporary directories created in /opt/apps/verodin/node/node/db/ff/jobs/ and job_actions directories were not successfully being cleaned up resulting in performance issues
- Fixed an issue where Director planner/tmp was consuming excessive disk space as Director version upgrade packages and patches were not being properly removed
- Fixed an issue where content for McAfee ESP was incorrectly being mapped as McAfee DLP
- Fixed an issue that prevented proper parsing of a PCAPNG file with an ethernet header

Known Issues

- OVA Directors have the ability to update Preview Integrations. Non-OVA Directors will be able to update Preview integrations in a coming release.
- The Multisite Reporting feature and Preview Integrations service are not working properly with RHEL8 Directors. We are working to resolve this issue as soon as possible.
- Local Event Filtering works as expected but is limited to Match Action, Match Integration, and Match Events (when the latter involve Raw Events). If a rule has a Match Event condition for any field other than Raw Event, the rule does not apply to Local Events. It only applies to events from standard local integrations in MSV.

Appliance OS Security Update

The latest platform security update can always be found on the [Validation Section of the Docs Portal](#) (<https://docs.mandiant.com/home/msv-security-patch-downloads>). This security update applies to all versions of the product and is cumulative.

Important Installation Notes

Minimum Director version 4.10.0.0 or higher is required to upgrade to version 4.12.1.0.



As of Actor version 4.12.0.0, we have ended support for Actors on 32-bit architectures, as well as the following OSes: Windows 7, Windows 8.1, Windows Server 2012 R2, and MacOS 10.14 Mojave. **Contact support** (<https://docs.mandiant.com/home/mandiant-support-cases>) if you have any questions or concerns.

In the meantime, you must take the following actions:

- Retire any Endpoint Actors on these platforms
or
- Replace the Actors with ones on supported platforms