Mandiant

PRODUCT UPDATE 4.14.6.0 - MAY 12, 2026

The Mandiant Security Validation (MSV) team is pleased to announce version 4.14.6.0 of the MSV platform.

Enhancements

- Updates to Director and content to support MITRE ATT&CK v18.
- Added support for Remote Integrations on installable Actors.
- MSI version downgrades are prevented on Director upgrades.
- For external database scenarios, upgraded the database encryption to support scram-sha-256 password hashing.
- Improved memory performance for the `/analyze/pivot_data` route.
- To enhance privacy, Azure Client Secrets used for Cloud Validation Modules (CVM) have more redactions.
- Added a setting to allow administrators to disable the requirement for a local user account when using Google or SAML authentication. That way, all users can use the selected authentication type without needing a local fallback.
- Updated API calls for the CrowdStrike Intel Threat Intelligence Platform integration to align with the latest CrowdStrike API endpoints.
- Improved Job Results page polling mechanism to reduce load on the Director backend.
- Improved Mitre Dashboard statistic population for certain Tactics.
- Enhanced job tagging to ensure that Jobs created through Monitors or Bulk Actions inherit the tags from the parent configuration.

Bug fixes

This release includes a number of bug fixes and stability improvements. Key fixes are categorized as follows:

Stability

- Fixed an issue causing leaking CLOSE_WAIT sockets in the Content API Service.
- Fixed an issue where RHEL actor upgrades to 4.14.5.0 would fail.
- Fixed an issue where the 4.14.5.0 Director Installer would fail with pgdg repository error messages.
- Fixed an issue where Protected Theater was generating new interfaces for vnetXX.
- Fixed an issue where the Director would return a 200 status even when sent a bad payload.
- Fixed an issue where date input to MSI test queries was not applied if defaults were left alone.
- Fixed a `NoMethodError: undefined method "extra_sleep"` error.
- Fixed a parse error in v2 MonitorDefsController, expecting JSON but finding a string.
- Corrected `vstatus` to report the status of the `valkey` service, not `redis`.
- Addressed an issue to restrict the size of logs that are created for Google Cloud Hosted Directors.
- Fixed an issue that prevented Cloud Evaluations from being run as a bulk action.
- Fixed an issue where scheduled jobs would sometimes not run and not appear in the job status.
- Fixed an issue where Cloud Profiles were not retained when rescheduling a previously cancelled scheduled Cloud Action using "Run Again".
- Fixed an issue that resulted in a 500 internal server error when updating Actor settings.

Security and authentication

- Fixed an issue where Azure Client Secrets used for Cloud Validation Modules (CVM) weren't fully redacted.
- Addressed a PostgreSQL authentication error: FATAL: Ident authentication failed for user "admin".
- Fixed an issue where potentially-sensitive fields weren't redacted when expanding the action job page.

Web interface

- Fixed an issue where a TrustedHTML/TrustedScriptURL Javascript error would appear.
- Fixed an issue where Action statuses were not updating after manually modifying events.
- Fixed an issue that prevented the scheduling of Job Reports on a past date.
- Fixed an issue where closing action details in a report builder report required clicking close several times.

- Fixed an issue where the Security Technology icon in Job Action Events failed to render.
- Fixed an issue where the heatmap was not showing the matrix table according to the configured rows and columns.
- Fixed an issue where running an action from the preview page failed to redirect to the job page and did not update the job status correctly.
- Removed help text regarding repository choice within the Actor Installer.

Known issues

- Local Event Filtering works as expected but is limited to Match Action, Match Integration, and Match Events (when the latter involves 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.
- Network configuration may reset unexpectedly. To resolve the issue, run `vsetnet` after the upgrade with static IP addresses for one or more interfaces.

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 4.14.0.0 or higher is required to upgrade to version 4.14.6.0.

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)**. For full details on how to upgrade, see **Updating Security Validation Components (https://docs.mandiant.com/home/msv-system-updates)**.

Failed upgrade from Director web interface

If your Director fails to upgrade to this version after you attempt the upgrade from the web interface, check **Troubleshoot failed upgrades (https://docs.mandiant.com/home/msv-failed-upgrade-41450)** for additional self-help tips. That document contains which log file to check, for what specific content, and how to use the provided script to fix the issue.