Mandiant

PRODUCT UPDATE 4.14.4.0 - SEPTEMBER 4, 2025

The Mandiant Security Validation (MSV) team is pleased to announce version 4.14.4.0 of the MSV platform.

Enhancements

- Adjusted Report Builder to work with sub-dimensions.
- Upgraded nginx SSL directive.
- Added additional Alternate name support for Actors to match multiple possibilities in the security controls and SIEM.
- Added MFA Registration Status in the User Management page.
- Upgraded the inetsim image in Protected Theater.
- Updated Actors to OpenSSL3.
- Updated reported Actor OS information in Director web interface.
- Newly-released Actor images have an `/opt` location with 20 GB of space.
- MSV requires encryption in the `database.yml` file using `vconfigdb` or `vsetdb` without providing a root certificate.

Bug fixes

- Fixed an issue where Directors showed an error when trying to pull content through an NTLM proxy connection.
- Fixed an issue where IPTables were not kept after an upgrade.
- Fixed an issue where Directors did not allow changes to capitalization of a user account.
- Fixed an issue where AEDA Monitor intermittently stalled, making Actors unusable.
- Fixed an issue where changing Pass/Fail criteria did not work.
- Fixed an issue where an expired password did not prompt a user for a password update.
- Fixed an issue related to scheduled Jobs on Windows Endpoint Actors.
- Fixed an issue where a Protected Theater upgrade completed, but new snapshots did not work.
- Fixed an issue where a Director stopped working when `/var/log` ran out of space.
- Fixed an issue where Run Again or Monitor (to create AEDA) didn't populate with all Action configurations.
- Fixed an issue where customers were unable to edit and save changes to an existing Google Chronicle Backstory integration.
- Fixed an issue where an Azure Sentinel integration was unable to match events with Phishing action.
- Fixed an issue where an Action with an authenticated interactive session failed to execute.
- Fixed an issue where the Threat Connect Integration was using basic authentication through proxy.
- Fixed an issue where a Red Hat Linux Enterprise Actor stopped working after registering to the Director.
- Fixed an issue where a Protected Theater Actor returned an error after multiple Actions were run.
- Fixed an issue where an MSI Splunk Integration matched events for the 127.0.0.1 IP address.
- Fixed an issue where content import did not show file count.
- Fixed an issue where file names were inconsistent when exporting reports through the Report Builder PDF compared to the report template or graphics.
- Fixed an issue where events from Palo Alto MSI integration were not matching to a security technology in the same way as the legacy integration.
- Fixed an issue related to the verodin_msi_log containing too much information and thus taking up too much space.
- Fixed an issue where correlation queries were not appearing under the MSI integration test view.
- Fixed an issue with PCAP imports running over port 80.
- Fixed an issue where the Action library showed the wrong date for a content application.
- Fixed an issue where the Report Builder wasn't reporting correctly on Managed File Transfer (MFT) Actions.
- Fixed an issue where the Report Builder Action Type filter used the incorrect value for website Actions.
- Fixed an issue where an Actor could not be upgraded because of insufficient disk space in the `/opt` partition.

- Fixed an issue where the **Check for Updates** in the Director web interface wasn't working.
- Fixed an issue where Gauges Reports were returning inaccurate data.
- Fixed an issue where an error was thrown while parsing the response from the LogRhythm legacy integration.

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 4.14.4.0.

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)**.