PRODUCT UPDATE 4.8.3.1 - MAY 24, 2022

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 4.8.3.1 of the platform. This release adds *improvements, and bug fixes.*

Important Installation Notes

- Minimum Director Version 4.6.3.0 or higher is required to upgrade to version 4.8.3.1.
- Actor Compatibility. Actors must be upgraded to at least version 4.6.0.0 before updating their Director to 4.8.3.1.

To download documentation, appliances, software, and updates, visit the **Validation Customer Portal (https://msv.mandiant.com/)**.

New Features and Updates

- The MSV Integration with ElasticSearch now supports TLS/SSL PKI Authentication.
- Proxy Assignments are now supported for Palo Alto integrations.

General Improvements

- Intermittent issues involving errors generated after the first group of actions is executed within protected theater have been resolved.

Bug Fixes

Issue key	Summary
MSV-4385	Actors encounter a MemoryError when processing a “pull_logfiles” action
MSV-4016	Actor does not parse passwords correctly during file_transfer actions
MSV-2747	HTTP Status 500 & Exception encountered when accessing /jobs/index_table_data.csv
MSV-3672	Sleep Actions within a group of DNS Actions breaks the start / end time which breaks event matching

Appliance OS Security Update

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 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.

	Director	Actor	Protected Theater
Critical	0	0	0

	Director	Actor	Protected Theater
High	3	3	4
Medium	0	0	0
Low	0	0	0

Details for the High severity vulnerabilities are as follows:

- CentOS 7 : firefox (CESA-2022:1703) (PT only)
- CentOS 7 : gzip (CESA-2022:2191)
- CentOS 7 : kernel (CESA-2022:4642)
- CentOS 7 : zlib (CESA-2022:2213)

You have two options for installing this security update:

- Via the MA-SV GUI, using a Patch file (verodin_sec_update_4.8.3.1.patch).
- Via the command line, using a tar.gz file (verodin_repo_4.8.3.1.tar.gz).

Instructions for applying the Security Update can be found in Chapter 5.5 of the Admin Guide.

Important Upcoming Changes

The following changes will be made in an upcoming release. Customers are advised to review and prepare for these changes:

- Reminder: Customers with MSV Licenses issued or renewed after January 1, 2022, are *required* to execute version 4.8.1.0 or later and maintain a connection to the Mandiant Content Service.
- The https://update.verodinservices.com URL and IP will be retired. Customers will need to ensure their ACLs are updated prior to this change to include the URLs listed below. The exact date of this cutover will be shared in a subsequent update.
    - https://update.validation.mandiant.com
    - https://content.validation.mandiant.com
    - https://telemetry.validation.mandiant.com
- The use of Integration Event Filters is discouraged, as it will no longer be available or supported in an upcoming release. You should recreate these filters using the new Event Suppression functionality. If that is not possible, please contact your TSC or **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.