Mandiant

# PRODUCT UPDATE 4.8.3.0 - APRIL 26, 2022

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 4.8.3.0 of the platform. This release adds several new and enhanced capabilities to the Validation Platform, including ***Report Builder enhancements, the ability to re-attach Actors, user experience improvements, and bug fixes***.

## Important Installation Notes

- **Minimum Director Version**. Director version 4.6.3.0 or higher is required to upgrade to version 4.8.3.0.
- **Actor Compatibility**. Actors must be upgraded to at least version 4.6.0.0 before updating Director to 4.8.3.0.

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

### General Enhancements

- When updating the VID for an Action via API or UI, if it is a PCAP Action, the PCAP name will change to VID.
- Queue optimization so that timeout Actions and Actions that have been pulled from the Director no longer show up in the queue.
- Added the ability to tune the frequency of polling for status updates during job Actions on the Director.
- Additional debug logging for future troubleshooting capabilities.

## General Improvements and Bug Fixes

Minor bugs and usability issues were resolved, including reliability improvements for dashboards and PDF report improvements.

## Appliance OS Security Update

The MA-SV 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 | | | |
| High | 2 | 1 | 2 |
| Medium | 1 | 1 | 3 |
| Low | | | |

Details for the High severity vulnerabilities against the Director are as follows:

- CentOS 7 : expat (CESA-2022:1069)
- CentOS 7 : httpd (CESA-2022:1045)

Details for the High severity vulnerabilities against the Actor are as follows:

- CentOS 7 : expat (CESA-2022:1069)

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

- CentOS 7 : expat (CESA-2022:1069)
- CentOS 7 : firefox (CESA-2022:0824)

### Updated Information about Appliance OS Security Updates

There are three options available for installing updates to the appliance OS:

- By enabling automatic updates on appliances
- Via the MA-SV GUI, using a Patch file (verodin_sec_update_4.8.3.0.patch).
- Via the command line, using a tar.gz file (verodin_repo_4.8.3.0.tar.gz).

For full details, see the new "Validation Appliance OS Security Updates" tech brief or the Security Patch section of the Admin Guide (Chapter 5.5).