CAWS 3.1 Release Notes

CAWS Continuous Security Validation Platform

Version 3.1

1. Introduction

This document communicates the major new features and changes in this release of CAWS 3.1. It also documents known problems and workarounds.

2. Compatible Products

This release has been tested on the following browsers and operating systems:

- Google Chrome on:
  - Windows 7 SP1
  - Windows 8.1
  - Windows 10
- Microsoft Edge on:
  - Windows 10
- Google Chrome and Safari on:
  - OS X Sierra 10.12

3. New Features

3.0 Release

New Features

The following new features added in the release:

- New UI:
  - Better representation of data and trend analysis.
  - Improved Visualization of Threat Intelligence.
  - Improved Visualization of Chain of Events.
  - Improved Search and filtering of data.
  - Improved performance and response time.
- **Payload Scoring**: Updated algorithm that takes malware drops into consideration when determining exploits missed by security products.
- **New and Improved API**: A new and improved API that provides the ability to define precisely the data you want — and only the data you want— resulting in new possibilities and workflows that are freed from the limitations of downloading and parsing massive JSON blobs.
- Support for file based exploits.
- Application is hosted on Cloud for better performance.
- Enhanced Threat Information, Including improved geolocation associations.

3.1 Release

New Features

Following new features added in the release:

- **Payload Scoring**: Updated algorithm that takes malware drops into consideration when determining exploits missed by security products.

Enhancements

Following bug fixes have been included in the release

- Issue with loading NSS-Id details failing when the calendar has older date range than NSS-Id being used from search has been addressed.
- Error message is now displayed when an invalid NSS-Id is queried.
- Hide create account button and account details for account viewer user.
- Update organizations/account data after edit account.
- Prevent access to file and URL submissions if user is not associated with an org or account.
- Updated Organization and accounts page for better usability.
- Added tooltips for more obvious error messaging.
- Added Login UI progress indicator for better user experience.
- Hiding the create profile link in profile list when 0 profiles exist for viewer role.
- Removed unnecessary fields from email template.
- Added reversed date time sort so that the latest dates are returned before earlier dates by default.
- Submission URLs are now being encoded.

4. Known Limitations and Changed Behavior in this Release

The following feature have been deprecated:

- Risk Modeling
- Layered Defenses

The following limitations exist in this release:

- Geolocation data is not available for exploits found before April 14, 2017. The exploits will not be visible on the map for any date prior to April 14, 2017.
- Threat bypass notifications feature is not available in CAWS 3.0.
- Chrome login sessions does not timeout automatically.
- Filters on Global Dashboard or Threats may have zero results and UI does not display any data in that case.
- An active session will be terminated when user tries to login from a different PC or different browser.
- UI Layout might have some issues with scaling down on small screens.
- Random display issues with Exploit Chain of Events.
- Map in Analyze section does not load properly on Firefox browser.
- An account can have a maximum of 75 security profiles.
- CAWS-1161: Sorting of list items in various views using the headers is not available.
- CAWS-855: Unable to copy the text from search results list.

- CAWS-852: Global search needs the complete string (NSS-ID, MD5Hash or URL etc.) and partial search feature is not available.
- CAWS-479: Changing data range on global dashboard and threats section resets all filters.
- CAWS-1363: Inactive user account not visible on User Accounts tab in organizations.
- CAWS-1350: Searching for NSS-IDs is case sensitive.