Release Notes: Mac Sensor v6.2.7

January 2020

Summary

CB Response Mac Sensor v6.2.7 provides Mac Keychain storage implementation, strict mode for certificate validation, network isolation exceptions, bug fixes and stability improvements. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to CB Response Mac Sensor v6.2.6 from previous versions as well as users new to CB Response. The key information specific to this release is provided in the following major sections:

- **Installation Instructions** - Provides instructions for Mac Response sensor installation.
- **New features** – Describes new features introduced in this release.
- **Corrective content** – Describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations** – Describes known issues or anomalies in this version that you should be aware of.

Server compatibility

Cb Response sensors included with Cb Response server releases are compatible with all server releases going forward. It is always recommended to use the latest server release with our latest sensors to utilize the full feature capabilities of our product, however, using earlier 6.x server versions with the latest sensor should not impact core product functionality.

Sensor operating systems

CB Response sensors interoperate with multiple operating systems. For the most up-to-date list of supported operating systems for CB Response sensors (and all Carbon Black products), refer to the following location in the Carbon Black User eXchange:
https://community.carbonblack.com/docs/DOC-7991

Documentation

This document supplements other Carbon Black documentation. Click here to search the full library of CB Response user documentation on the Carbon Black User eXchange.

Technical support

CB Response server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that might develop during the installation or upgrade process. Our Professional Services organization is also available to assist to ensure a smooth and efficient upgrade or installation.

Note: Before performing an upgrade, Carbon Black recommends reviewing content on the User eXchange for the latest information that supplements the information contained in this

document.

Installation Instructions

To install the sensors on to your server, run through the following instructions:

1. Ensure your CB Response YUM repo is set appropriately:
    a. The CB Response repository file to modify is */etc/yum.repos.d/CarbonBlack.repo*
    b. Baseurl = https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
2. On the CB Response server, clear the YUM cache by running the following command:
    a. *yum clean all*
3. After the YUM cache has been cleared, download the sensor install package by running the following command:
    a. *yum install --downloadonly --downloaddir=<package local download directory><package>*
        i. **Note:** The *<package local download directory>* is a directory of your choice
        ii. **Note:** *<package>* is replaced by *cb-osx-sensor*
4. Install the new sensor package on the CB Response server by running the command:
    a. *rpm -i --force <package downloaded>*
5. Make the new installation package available in the server console UI by running the command:
    a. */usr/share/cb/cbcheck sensor-builds --update*
        i. **Note:** If your groups have *Automatic Update* enabled, the sensors in that group will start to automatically update.

Your new sensor versions should now be available via the console. For any issues, please contact Carbon Black Technical Support.

New Features

- **Network Isolation Exceptions** - This feature allows CB Response users to add a set of IP addresses or URLs to exclude from network isolation on a per sensor group basis. Threat Hunters & Incident Responders can allow IT tools, VPN and proxy connections, and other security tools to continue to operate while putting the sensor in isolation. [CB-27684]
- **Mac Keychain Storage** - In an effort to increase sensor hardening, sensitive data related to the Mac Response sensor will now be stored in the Mac Keychain. By utilizing the Keychain, you can be confident that the Developer ID-signed builds that Carbon Black distributes only retains sensitive sensor configuration data using best practices recommended by the platform vendor for storing and setting configuration options. This will also allow for stricter certificate validations in the future, as well as certificate creation and swapping using the Keychain Manager class. [CB-24369]
- **CB Live Response Improvements** - Added additional customization for CB Live Response file chunk size using “Get” command for improved transfer speeds in various bandwidth environments. [CB-25917]
- **Strict Certificate Enforcement** - You can require stricter validation of certificates so that if a server certificate used by a sensor fails standard X509 certificate validation checks (excluding revocation), server-sensor communication will be disabled. [CB-24368]

Corrective Content

This release provides the following corrective content changes:

- Added Mac Keychain storage feature and functionality for sensor hardening. [CB-24369]
- Fixed bug with driver reload failing to reset the sensor health score. [CB-26750]
- Fixed bug to report local IP and port information in server UI for TCP connections for IPv4 and IPv6. [CB-13162]
- Added ASLR functionality so memory used is not mapped to an explicit address. [CB-24385]
- Updated sensor compilation to enable stack-based buffer overflow protection. [CB-24387]

Known Issues and Limitations

Known issues associated with this version of the sensor are included below:

- Downgrading from v6.2.7 to previous sensor versions will require a reinstallation due to changes in the way the sensor database is accessed. More information can be found at the UeX post here:

https://community.carbonblack.com/t5/CB-Response-Discussions/Mac-Response-Manually-Downgrading-from-6-2-7-osx-Sensor/m-p/84574#M4343 [CB-28154]

- The Original Filename and Product Name for the CommCenter binary on MacOS is not being properly captured in the Server UI. [CB-17611]
- If you disable path exclusions in *cb.conf* you must reboot the system to update the previous path exclusion settings preserved in cache. [CB-14660]
- The Mac Response sensor does not store Live Response activity in the *sensor.log* file by default. Users can monitor Live Response activity using the *live-response.log* found under */var/log/cb/audit* on the Response server. Additionally, users can enable more verbose logging of the *sensor.log* file to capture Live Response activity on the Mac endpoint. Please note, enabling verbose logging may quickly consume the specified *sensor.log* size and should be used cautiously as enabling may lead to shorter retention of audit information. This verbose logging can be enabled by modifying the *logging.config* file under */var/lib/cb* to to set the following parameters: *minloglevel: 0*, *V:0*. [CB-8908]

Contacting Support

Use one of the following channels to request support or ask support questions:

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When contacting Carbon Black Technical Support, be sure to provide the following required information about your question or issue:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (CB Response server and sensor version)
- **Hardware configuration:** Hardware configuration of the CB Response server (processor, memory, and RAM)
- **Document version:** For documentation issues, specify the version and/or date of the manual or document you are using
- **Problem:** Action causing the problem, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request