Release Notes: Windows Sensor v6.2.1

November 2018

Summary

Cb Response Windows Sensor v6.2.1 includes major new functionalities, bug fixes, and stability improvements. This sensor release also includes all changes and fixes from previous releases.

For the latest stable maintenance release please consider installing Windows Sensor v6.1.9.

This document provides information for users upgrading to Cb Response Windows Sensor v6.2.1 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:

- **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. However, they are incompatible with Cb Response server releases prior to the version they shipped with.

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 new sensor, perform the following steps:

1. Ensure your yum repo is set appropriately: modify /etc/yum.repos.d/CarbonBlack.repo with the appropriate baseurl, if needed.
    - Baseurl=https://yum.distro.carbonblack.io/enterprise/6.2.4-1/x86_64
    - Run yum install --downloadonly --downloaddir=<local directory to download the package into> <package>
    - <package> is replaced by cb-sensor-6.2.1.81002-win
2. Run the following command to install the package:
    - **rpm -i --force** <*package*> (current package to use: *cb-sensor-installer-6.2.1.81002-win-noarch.rpm)*
3. Run the following command to make the new installation package available in the server console UI:
   Note: If your groups have Automatic Update enabled, the sensors in that group will start to automatically update.
    - **/usr/share/cb/cbcheck sensor-builds --update**

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

New Features

- The Cb Response Windows Sensor is now FIPS Compliant
    - Configurations for specific OS Versions
        - Windows XP and Windows Server 2003 requires a server configuration to enable TLS 1.0 for on-prem environments
            - https://blogs.msdn.microsoft.com/kaushal/2011/10/02/support-for-ssltls-protocols-on-windows/
            - For cloud environments, please reach out to support for TLS 1.0 enablement.
        - Windows Vista and Windows Server 2008 requires TLS 1.2 to be configured for on-prem and cloud environments
            - https://support.microsoft.com/en-us/help/4019276/update-to-add-support-for-tls-1-1-and-tls-1-2-in-windows
        - Windows 7 and all releases that follow do not require any further configurations.
    - Turn FIPS on/off by:
        1. Press Windows Key+R to open Run dialog.
        2. Type “regedit” into the Run dialog box (without quotes) and press Enter.

3. Navigate to "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\".
4. Look at the "Enabled" value in the right pane. If it's set to "0", FIPS mode is disabled. If it's set to "1", FIPS mode is enabled. To change the setting, double-click the "Enabled" value and set it to either "0" or "1".
5. Restart the computer.

- Cb Response now supports SHA-256 Hash Reporting

Corrective Content

This release provides the following corrective content changes:

- Fixed issue with sensor.log file displaying an IP address as an integer instead of a quad decimal [CB-21591]
- Resolved issue where the sensor does not update it's sensor id when requested to do so be the server [CB-21221]
- Fixed issue where device path transform/normalize was incorrect [CB-21050]
- Mitigated issue for when drive letter is missing from the drive path after modload events and captured and sent to the Cb Response Server [CB-20881]
- Resolved bug, allowing for sensor to resolve server's address before deciding which local IP to use for process-related events. [CB-20452]
- Throttle rates can now be manually removed and are now lifted when the throttle time window expires. [CB-19852]
- Fixed higher than expected CPU of sensor not successfully registered with the server. [CB-19178]

Known Issues and Limitations

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

- **Disabling DNS Name Resolution For NetConn Events:** Customers have observed that the Windows sensor can report high CPU utilization by the Carbon Black service ('cb.exe') on machines with a continually large number of network connections (e.g. DHCP/DNS servers, Domain Controllers, etc.). To help alleviate the high CPU utilization, without having to disable collection of network connection events, the windows sensor can be configured to disable DNS name resolution in data collection for network connection events by configuring the windows registry key:

  [HKEY_LOCAL_MACHINE\SOFTWARE\CarbonBlack\config]

  "DisableNetConnNameResolution"=dword:00000001

- **Cb Entries Remaining in Add/Remove Programs:** Customers uninstalling their Cb Response Windows sensor through uninst.exe will notice remaining Cb entries in the Add/Remove Programs window.xcxz

- **Cb Branding Is Different Between MSI and EXE Installers:** Customers using the Add/Remove Program window to manage their Cb Response installation should be aware that the Cb branding between the MSI and EXE installers is different.
- **Disproportionate Cb Logo on Install Wizard:** Customers running the .exe installer may notice a disproportionate Carbon Black logo appearing on the Install Wizard
- **Install/Uninstall & Upgrade/Downgrade of Sensor on WinXP & WinServer2003 Requires Reboot:** Customers running the Windows sensor on a Windows XP or Windows Server 2003 machine should note that a reboot of the machine will be required for all install/uninstall and upgrade/downgrade methods in order to successfully load and unload Cb drivers.
- **Cb Protection Upgrade Needed:** Customers who are running Cb Protection to tamper protect the Cb Response Sensor and do not opt-in to CDC will need to update their tamper rule settings for Cb Protection to the latest "Cb Response Tamper Protection" Rapid Config (if running CbP 8.0) or Updater (if running CbP 7.x) in order to successfully upgrade/downgrade their Cb Response sensor. Please contact technical support to obtain the latest Rapid Config or Updater for CbP.

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