VMware Carbon Black EDR

# Release Notes: Windows Sensor v6.2.5

February 2020

## Summary

VMware Carbon Black EDR Windows Sensor v6.2.5 is intended to provide improvements to Windows memory dumps, capturing of the logon type for Windows process executions, support for Flash and Microsoft Link file types, additional Tamper Hardening, performance improvements to our Network Isolation feature, stability improvements and bug fixes. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to VMware Carbon Black EDR Windows Sensor v6.2.5 from previous versions as well as users new to VMware Carbon Black EDR. The key information specific to this release is provided in the following major sections:

- **Installation Instructions** - Provides instructions for VMware Carbon Black EDR Windows 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

VMware Carbon Black EDR sensors included with 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 server versions with the latest sensor should not impact core product functionality.

## Sensor operating systems

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

## Documentation

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

## Technical support

VMware Carbon Black EDR 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, VMware 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 VMW CB EDR YUM repo is set appropriately:
    a. The VMW CB EDR 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 VMW CB EDR 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. Run *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-sensor-6.2.5.91203-win*
4. Install the new sensor package on the VMW CB EDR server by running the command:
    *a. rpm -i --force <package>*
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 VMware Carbon Black Technical Support.

**Important Note:** Installations and upgrades (as well as uninstallations and downgrades) of the sensor on Windows XP and Windows Server 2003 **will require a reboot** in order to properly load (or unload) our software drivers.

For all other Windows OS, it is always encouraged to conduct a reboot of the endpoint after installation (or restart) of our sensor to ensure the sensor properly captures the full historical data of all running processes and associated information.

# New Features

- **Network Isolation Improvements** - The v6.2.5 Windows sensor improves performance of our sensors packet filtering techniques to allow for higher network throughput, especially in virtualized environments. [CB-27931]
- **Windows Memory Dump Improvements** - In conjunction with the 7.0.0-svr, the v6.2.5 Windows sensor will compress memory dump files created through Live Response by default. In addition, the Windows sensor provides a full “raw” memory dump on Windows 10 systems where the “Virtual Based Security” setting may be enabled. [CB-27702]
- **Tamper Hardening Improvements -** The v6.2.5 Windows sensor provides additional Tamper Hardening. [CB-26653]
- **Capturing Logon Type for Windows Process Executions** - The v6.2.5 Windows sensor now captures “logon type” associated with Windows process executions. [CB-27714]

# Corrective Content

This release provides the following corrective content changes:

- Fixed a bug where running the Live Response execfg command could generate large temp file sizes. [CB-27472]
- Fixed a bug where the “Tamper Type” source information was not being populated for certain tamper alerts. [CB-27698]
- Fixed a bug where netconn events of Isolation excluded URLs were not reported under the process analysis page. [CB-28100]
- Corrected some grammar in the GPO_README.txt file. [CB-28112]
- In conjunction with the 7.0.0-svr, the v6.2.5 Windows sensor now computes and stores file hash information for Flash (.swf) and (.flv) as well as Microsoft Link files (.lnk). [CB-28185]
- Fixed a bug with the sensor attempting to resolve bogus IP addresses. [CB-28213]
- Fixed a bug causing high CPU usage with normalizing file names. [CB-28353]

- Fixed a bug causing BSODs when the filter driver is unloaded. [CB-28355]
- Fixed a bug with the sensor modifying a non-ASCII hosts file. [CB-28482]
- Fixed a bug causing BSODs when the filter driver fails to load properly. [CB-28531]
- Improved sensor diagnostics to capture TLS settings from Windows Registry. [CB-28533]
- Fixed a bug with the RawEventStats.log file generating an INVALID row. [CB-28630]
- Improved sensor logging of health score related events. [CB-28631]
- Updated sensor to prevent installation on non-supported operating systems including Windows XP and Windows Server 2003. See our UEX post for more information. [CB-28638]
- Fixed a bug with the sensor failing to apply non-default debug levels at startup. [CB-28673]
- Improved sensor to limit high event loss in heavy workload situations. [CB-28674]
- Improved the sensor to search for existent ETL sessions before beginning a new session for better sensor log retention. [CB-28834]
- Fixed a bug impacting endpoint performance during file rename and delete operations on a network share. [CB-28844]
- Fixed a bug where non-server upgrades may fail due to a missing certificate. [CB-29055]
- Fixed a bug causing BSODs when reporting certain Tamper related events. [CB-29095]
- Fixed a bug with sensors installed via MSI leaving behind artifacts when uninstalled through the server UI. [CB-29181]
- Fixed a bug with uninstalling the sensor through Add/Remove Programs leaving behind artifacts. [CB-29258]

# 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 [CB-17552]:

  [HKEY_LOCAL_MACHINE\SOFTWARE\CarbonBlack\config]

"DisableNetConnNameResolution"=dword:00000001

- **Tamper Detection Events Generated When Restarting Sensor Service from Response Server:** Customers restarting the sensor service from the server console, with Tamper Detection enabled, will observe Tamper Detection alerts that will be assigned to the cb.exe process of the outgoing process. [CB-21882]

- **Obfuscated Windows Sensors Will Not Start After First Reboot:** Windows sensors installed from an obfuscated sensor group will not start after first reboot. A second reboot will start the sensor service. [CB-28062]

- **CB Entries Remaining in Add/Remove Programs:** Customers uninstalling their CB EDR Windows sensor through uninst.exe will notice remaining CB entries in the Add/Remove Programs window. [CB-28059]
- **CB Branding Is Different Between MSI and EXE Installers:** Customers using the Add/Remove Program window to manage their CB EDR Windows sensor installation should be aware that the CB branding between the MSI and EXE installers is different. [CB-28063]
- **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-28261]
- **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.x) 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. [CB-15941]

# 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