Release Notes: Windows Sensor v7.2.0

December 2020

Summary

VMware Carbon Black EDR Windows Sensor v7.2.0 is intended to provide support for our new *Tamper Protection* feature in addition to bug fixes and other improvements. 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 v7.2.0 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.
- **Contacting Technical Support** – Describes ways to contact Carbon Black Technical Support and what information to have ready.

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-7.2.0.17354-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: 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

This release provides the following new feature content:

- **Tamper Protection:** Tamper Protection provides more security to the EDR Windows sensor by blocking local admin attempts to inject, remove, modify, or delete the sensor by protecting the sensor service, drivers, files, folders, registry settings and other sensor components. Please see the *VMWare Carbon Black EDR 7.4 User Guide* for more information. Tamper Protection requires a minimum Operating System version of Windows 10 v1703 (Desktop) or Windows Server v1709. In addition, Tamper Protection requires minimum versions of both the Windows 7.2.0 sensor and 7.4.0 EDR Server. [CB-27655]

Corrective Content

This release provides the following corrective content changes:

- Fixed a bug with installing .EXE over .MSI causing two Add/Remove Program entries. [CB-13313]
- Fixed a bug with Windows Registry entries remaining after sensor uninstall for sensors installed via the MSI package. [CB-24968]
- Fixed a bug with Add/Remove Program entries remaining after sensor uninstall. [CB-28059]
- Fixed bug with reporting hashes observed on remote volumes. [CB-30039]
- Improved driver diagnostics. [CB-30168]
- Fixed bug with Tamper Level value in HKLM\Software\CarbonBlack\config. [CB-30187]
- Fixed a bug with CB EDR Windows entries remaining in hosts file after uninstallation. [CB-30779]
- Fixed a bug with collecting modinfo events for binaries observed while collection was disabled. [CB-30893]
- Updated Osqueryi.exe to version 4.5.1. [CB-31578]
- Removed support for the “-remember” parameter for sensordiag.exe. [CB-31903]
- Fixed a bug causing a resource leak. [CB-31959]
- Fixed a bug where “CbEDRAMSI.dll” was not being uninstalled on sensor downgrades to versions prior to 7.1.0-win. [CB-32057]

- Fixed a bug with adding/removing Windows Registry values for AMSI support on sensor upgrades/downgrades. [CB-32090]
- Updated product name and logo information to “VMware CB EDR (Windows)”. [CB-32146]
- Fixed a bug with Tamper alert reporting. [CB-32183]
- Fixed a bug with the Carbon Black EDR sensor version overriding the Carbon Black Cloud sensor version in the Program Files listing for endpoints with both products installed. [CB-32548]
- Fixed a bug with the Carbon Black EDR sensor overriding the Carbon Black App Control sensor in the Program Files listing for endpoints with both products installed. [CB-32617]
- Improved connection between cb.exe and cbstream driver. [CB-32806]
- Fixed a memory consumption issue with the service. [CB-32827]
- Fixed a bug with “CbEDRAMSI.dll” parent directory being created and unable to be removed for non-AMSI supported Windows OS. [CB-32966]
- Fixed a bug with AMSI extension that could lead to script failures for Powershell. [CB-33118]
- Fixed a bug with the sensor crashing on terminal servers. [CB-33250]
- Fixed a bug with “CbEDRAMSI.dll” being installed on non-AMSI supported Windows OS. [CB-33371]
- Improved Tamper Detection feature to provide additional Tamper hardening. [CB-33484]

Known Issues and Limitations

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

- **Disabling DNS Name Resolution For NetConn Events:** Versions of the sensor prior to 7.1.1 (and 6.1.12 for XP/Server2003) were susceptible to high CPU utilization in the IP Address-to-Hostname resolution functionality of the sensor. This issue has been addressed, however, this registry key will still disable IP address name resolution for customers who wish to do so. [CB-17552]:

  [HKEY_LOCAL_MACHINE\SOFTWARE\CarbonBlack\config]

  "DisableNetConnNameResolution"=dword:00000001

- **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 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]
- **Windows 10 v2004 May Decrement Sensor Health Score on Startup:** Users running Windows 10 v2004 may initially observe a decreased sensor health score related to "Excessive (or Very High) Event Loss" on startup due to an uptick of regmod events observed by the sensor during boot up for this particular OS version. The sensor health score will correct itself after a period of idle time. [CB-32896]
- **Carbon Black App Control "Tamper Protection" Rapid Config Update Recommended:** For users running Carbon Black App Control (formerly "CB Protection") to tamper protect the Carbon Black EDR Windows Sensor (and do not opt-in to CDC) it is recommended to update the tamper rule settings for Carbon Black App Control to the latest "Carbon Black EDR Tamper Protection" Rapid Config to avoid possible conflict with applying Tamper Protection enforcement on both EDR and App Control. Please note, enabling Tamper Protection on both App Control and EDR does not provide extra protection and it is recommended to disable App Control enforcement of Tamper Protection once EDR enforcement is confirmed to be in place. When running EDR in "Tamper Detection" mode, "Tamper Protection" through App Control is still recommended. Tamper Protection (for EDR) requires a minimum Operating System version of Windows 10 v1703 (Desktop) or Windows Server v1709. In addition,Tamper Protection (for EDR) requires minimum versions of both the Windows 7.2.0 sensor and 7.4.0 EDR Server. Please contact technical support to obtain the latest Rapid Config for CB App Control if needed. [EP-11934]

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 EDR server and sensor version)
- **Hardware configuration:** Hardware configuration of the CB EDR 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