Summary

CB Response Linux Sensor v6.1.10 contains stability and performance improvements as well as bug fixes. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to CB Response Linux Sensor v6.1.10 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** - Describes installation instructions of the linux sensor
- **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.

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/stable/$releasever/$basearch/
2. Clear the yum cache
    *   **yum clean all**
3. Download the installer
    *   Substitute the cb-linux-sensor-installer name for *<package>*
    *   The *<package local download directory>* is a directory of your choice (like /home or /tmp)
    *   Run the following command to download the installer
        yum install --downloadonly --downloaddir=*<package local download directory>* *<package>*
4. Change your directory to the <package local download directory> from step #3
5. Run the following command to install the package:
    *   **rpm -i --force** *<package>* (current package to use: *cb-linux-sensor-installer-6.1.10.10169.noarch.rpm)*
6. 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. If the following warning occurs:

*   warning: /tmp/cb-linux-sensor-installer-6.1.10.10169-1.noarch.rpm: Header V4 RSA/SHA1 Signature, key ID 6ac57704: NOKEY

check out this Knowledge Base Article: How to provide public key for Linux sensor package. For any other issues, please contact Carbon Black Technical Support.

Corrective Content

This release provides the following corrective content change:

*   Fix to prevent crashes See KB article here [CB-24294]

*   Fix for repeated segfaults causing core dumps. [CB-24152]

*   Cb Response Linux sensor no long gives excessive warning messages about forked child of pid 1 [CB-22557]

*   Provides improvements to stability and performance [CB-21916/CB-23722]

Known Issues and Limitations

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

- Upgrading to the v6.1.10 sensor can cause a system panic if certain other security software (i.e. Tripwire, McAfee) is also installed. A fix was introduced in v6.1.7. [CB-18026].
  Important: Since v6.1.7 fixed this issue, this cannot happen once you have successfully upgraded to a later sensor. If you have Tripwire or McAfee installed, you should unload it before upgrading CB Response Linux sensor or this will require a reboot. See https://community.carbonblack.com/docs/DOC-15629 for additional detail.

- The sensor does not install on Oracle 7.4 without the RHCK Kernel being installed first. [CB-18158]

- This version of the Linux Sensor Installer does not respect specification of a non-default installation directory in cb.conf on the server – the default directory is always used. [CB-17033]

- Memory and CPU usage in the cbdaemon increases as a systems becomes busier. Under certain workloads such as a long lived processes with lots of forked children the memory and cpu usage can become excessive. [CB-16064/CB-21648]

- PID reuse on the system may cause new processes to not be suppressed when they should be. [CB-19523]

- On RHEL/CentOS 6.x systems, upgrading sensors older than v5.2.13 and v6.1.3 cause a duplicate sensor to appear in the Server UI. See https://community.carbonblack.com/docs/DOC-10841 for additional detail and a link to a workaround that hides the older sensor from the UI. This is mitigated in RHEL/CentOS 7.x systems. [CB-19224]

- Some outbound UDP network connections are not reported on Linux platforms. [CB-6630]

- ICMP traffic is allowed when sensor is isolated on Linux and OS X platforms. [CB-6483/CB-6623]

- Non-binary file write event collection cannot be disabled on Linux platforms. [CB-6686]

- The Linux sensor may fail to generate an MD5 and collect a binary image of file on a network share or user-space file system. This may also fill glusterfs error log with messages. [CB-6749/CB-2185]

Contacting Support

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

Carbon Black.

- **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