CB RESPONSE

Release Notes: Linux Sensor v6.2.1

August 2019

The Linux Sensor v6.2.1 release notes contain the following sections:

Summary

CB Response Linux Sensor v6.2.1 introduces SUSE 12 and 15 together with RHEL 8 and 7.7. Carbon Black includes support for newer 4.4+ linux kernels on SUSE and RHEL8 using eBPF technology. On these systems, updates to your kernel must also include updates to your kernel-devel package. The directory structure is updated to better align with industry best practices and Common Criteria.

Important: Downgrades from 6.2.x to 6.1.x are not supported at this time.

Sensor operating systems

CB Response sensors operate with multiple operating systems. For the most up-to-date list of supported operating systems for CB Response sensors, see https://community.carbonblack.com/docs/DOC-7991.

Documentation

This document provides information for users who are upgrading to CB Response Linux Sensor v6.2.1 from previous versions, as well as users who are new to CB Response. 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.

Installation Instructions

To install the new sensor:

1. Set your yum repo 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 that you choose, such as `/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-6.2.1.10119-1.noarch.rpm`*)
6. Run the following command to make the new installation package available in the server console:
    - `/usr/share/cb/cbcheck sensor-builds --update`

    Note: If your groups have **Automatic Update** enabled, the sensors in that group will automatically update.

Your new sensor versions should now be available via the console. If the following warning occurs:

```
warning:
/tmp/cb-linux-sensor-installer-6.2.1.10119-1.noarch.rpm: Header
V4 RSA/SHA1 Signature, key ID 6ac57704: NOKEY
```

refer to this Knowledge Base Article: How to provide public key for Linux sensor package.

For any other issues, contact Carbon Black Technical Support.

New Features

SUSE Support

Introducing support for SUSE 12 SP2, SP3, and SP4 together with SUSE 15. Currently, isolation and banning are not supported with SUSE.

RHEL 8 Support

Introducing support for RHEL 8. Currently isolation and banning are not supported with RHEL 8.

RHEL 7.7 Support

Introducing support for RHEL 7.7.

eBPF

On systems that have 4.x kernels (RHEL 8+ and SUSE), the sensor kernel module is replaced by eBPF.

Directory Updates

In preparation for work related to Common Criteria, we've updated the directory structure to align Linux recommendations for storing and setting configuration options.

SUPPORT MATRIX	**Event Collection**	**Suppression**	**Live Response**	**Network Isolation**	**Hash Banning**
SUSE 15 / 4.12+ kernel + kernel-devel	6.2.x	6.2.x	6.2.x	Not Yet Supported	Not Yet Supported
SUSE 12 (SP2, SP3, & SP4) / 4.4+ kernel + kernel-devel	6.2.x	6.2.x	6.2.x	Not Yet Supported	Not Yet Supported
RHEL8 / 4.18.0 kernel + kernel-devel	6.2.x	6.2.x	6.2.x	Not Yet Supported	Not Yet Supported
RHEL7 / 3.10.0 kernel	6.1.x & 6.2.x	6.1.x & 6.2.x	6.1.x & 6.2.x	6.1.x & 6.2.x	6.1.x & 6.2.x
RHEL6 / 2.6.32 kernel	6.1.x & 6.2.x	6.1.x & 6.2.x	6.1.x & 6.2.x	6.1.x & 6.2.x	6.1.x & 6.2.x

Corrective Content

This release provides the following corrective content changes:

- Implement sensor log rotation. [CB-18921]
- Resolve cbdaemon crash when MALLOC_CHECK_ is enabled. The workaround documented in the following CB Knowledge Base article is no longer required: https://community.carbonblack.com/t5/Knowledge-Base/CB-Response-Linux-6-1-9-sensor-daemon-process-crashing/ta-p/65570 [CB-24303], [CB-25053], [CB-24394], [CB-24395], [CB-24717], [CB-27458], [CB-24261]
- Re-install runs correctly after a clean install. [CB-27150]
- Load all banned hashes at startup. [CB-26597]

Known Issues and Limitations

Known issues associated with this version of the sensor:

- **Downgrade from 6.2.x sensors to 6.1.x is not supported**. Sensor removal and reinstall is required to downgrade from 6.2.x to 6.1.x.
- Process banning and network Isolation are not currently supported on 4.x kernels.
- On a SUSE and RHEL8 installation, if the system goes idle, it is possible to see a health status of 50 in the server console. The health score will restore to 100 on its own.
- Upgrading to the v6.2.1 sensor might refuse to update if certain other security software (i.e. Tripwire, McAfee, Cylance) is also installed on RHEL-6/7. This does not apply to RHEL-8 and SUSE systems.

  Important: If you have Tripwire or McAfee installed, a reboot might be required. See https://community.carbonblack.com/docs/DOC-15629 for additional details.
- The sensor does not install on Oracle Linux without the RHCK Kernel being installed first. [CB-18158]
  - Installation is possible with kernel 4.4+, but is not yet supported.
- 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 system becomes busier. Under certain workloads such as 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 can cause new processes to not be suppressed. [CB-19523]
- On RHEL/CentOS 6.x systems, upgrading sensors older than v6.1.3 causes a duplicate sensor to appear in the server console. See https://community.carbonblack.com/docs/DOC-10841 for additional details and a link to a workaround. This issue 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 a 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 can fail to generate an MD5 and collect a binary image of a file on a network share or user-space file system. This can also fill glusterfs error log with messages. [CB-21851]
- CB might cause errors on remote file systems (such as NFS). [CB-28115]
- Unloading cbsensor module may cause some programs to exit. [CB-26764]
- The sensor might report an incorrect binary backlog. [CB-26518]
- Memory usage in the driver and daemon might increase as max pid increases. [CB-25622]

Contacting Support

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

Note: Before performing an upgrade, Carbon Black recommends reviewing content on the User Exchange for supplemental information.

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

When contacting Carbon Black Technical Support, provide the following required information:

- **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.