Release Notes: Linux Sensor v6.3.1

June 2020

The Linux Sensor v6.3.1 release notes contain the following sections:

Summary

CB EDR Linux Sensor v6.3.1 introduces RHEL and CentOS 7.8 support and improved process execution visibility for eBPF-based sensors. It is strongly recommended you upgrade to this version if you are on 6.2.1-lnx, 6.2.2-lnx, or 6.3.0-lnx and utilizing eBPF-based sensors.

Sensor operating systems

CB EDR sensors operate with multiple operating systems. For the current list of supported operating systems, see https://community.carbonblack.com/docs/DOC-7991.

Documentation

This document provides information for users who are upgrading to CB EDR Linux Sensor v6.3.1 from previous versions and users who are new to CB EDR. This document supplements other Carbon Black documentation. Click here to search the full library of CB EDR 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 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-6.3.1.10007-1.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.

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

```
warning:
/tmp/cb-linux-sensor-installer-6.3.1.10007-1.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

RHEL 7.8 Support

Introducing support for RHEL 7.8. During testing of the CB EDR sensor against the 3.10.0-1127 kernel, we discovered that command line parameters are now stored in a different location from where we previously retrieved them. Command line details are vital information in threat detection.

CentOS 7.8 Support

Introducing support for CentOS 7.8.

Corrective Content

This release provides the following corrective content changes:

- Occasionally the command line is seen with garbage reported. [CB-10598]
- Panic in _socket_recvmsg() due to page fault on user address [CB-30952]

Known Issues and Limitations

Known issues associated with this sensor version:

- When swapping certs, the sensor tries to connect to the cert first SAN. if the address name is not the FQDN it won't resolve. [CB-31146]
- Not capturing last argument in a variable arg list in RHEL 6/7 [CB-31219]
- Sensor accepts expired certificates in strict mode, but will close connections when using an expired certificate. [CB-30424]
- Proxy setting in sensorsettings.ini will not work with custom TLS certificate. [CB-30175]
- Updating from sensor version v6.1.6 and earlier could result in a system panic if certain other security software (Tripwire, McAfee) is also installed. v6.1.7 introduced a safety mechanism to prevent this panic. This can result in the sensor refusing to update to prevent a panic. An update will occur on the next system reboot. To upgrade without a reboot, review

https://community.carbonblack.com/docs/DOC-15629 [CB-12773] for alternate instructions and further technical analysis of the issue.

- The Oracle UEK is not supported. The RHCK kernel must be installed prior to installing cbsensor on Oracle Linux. [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 system becomes busier. Under certain workloads such as a long lived processes with lots of forked children, memory and CPU usage can become excessive. [CB-16064/CB-21648]
- PID reuse on the system can cause new processes to not be suppressed when they should be. [CB-18239/CB-29810]
- 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 console. See https://community.carbonblack.com/docs/DOC-10841 for a workaround that hides the older sensor from the console. This issue is mitigated in RHEL/CentOS 7.x systems. [CB-19224]
- ICMP traffic is allowed when a sensor is isolated. [CB-6623]
- Unloading the cbsensor module can cause some programs to exit due to an unexpected return from a socket read. [CB-26764]
- The sensor might report an incorrect binary backlog. [CB-26518]

Contacting Support

CB EDR 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 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.