VMware Carbon Black EDR

Release Notes: Linux v7.0.0

September 2020

The Linux Sensor v7.0.0 release notes contain the following sections:

- Summary
- Installation Instructions
- New Features
- Corrective Content
- Known Issues and Limitations
- Contacting Support

Summary

CB EDR Linux Sensor v7.0.0 introduces Ubuntu 18.04, Ubuntu 20.04, and Banning for eBPF. This release also introduces an open source version of our kernel module and eBPF sensors.

Also of note with this release, to align with RHEL 6 end of life plans, we're dropping support for RHEL/CentOS 6 versions. Support for these versions will still be available in our 6.3.x-lnx versions and we'll be releasing a long term support version later this year for RHEL/CentOS 6 specifically.

Once upgraded, any subsequent downgrades from 7.0.0-lnx to previous versions will require a manual uninstall and reinstall due to extensive architectural changes to our 7.0.0 version.

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 v7.0.0 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

Warning: EDR Linux Sensors versions 7.x do not support el6 distros (RHEL/CentOS 6.x). Attempting to upgrade el6 endpoints will result in a failed upgrade and the sensor will be left offline.

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-7.0.0.14291-1.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-7.0.0.14291-1.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

Ubuntu Support

We are introducing support for Ubuntu! Included in this release is 18.04 and 20.04. Future releases will support Ubuntu's LTS versions going forward.

Banning for eBPF

Inline with our kernel module support we're bringing hash banning to eBPF based sensors to include RHEL/CentOS 8+, SUSE, and Ubuntu.

Open Source

VMware Carbon Black EDR Linux is proud to announce our kernel module and eBPF code is now available as open source software under the GPLv2 license at https://github.com/vmware/cbsensor-linux-kmod and https://github.com/vmware/cbsensor-linux-bpf/ respectively.

The distributions supported by the kernel module are RedHat 6 and 7 and derivatives that use the same RedHat kernels (CentOS, Oracle Linux). eBPF supports RedHat/CentOS 8+ as well as SUSE 12 and 15, and Ubuntu 18.04 and 20.04. Also included with our eBPF code is an example script that runs basic Linux telemetry under a BSD 2-Clause.

Open sourcing these parts of our sensor enables us to work more closely with the security community to produce a better product. Community contributions will be included in future development of our VMware Carbon Black EDR Linux sensor.

Corrective Content

This release provides the following corrective content changes:

- Occasionally the command line is seen with garbage reported. [CB-10598]
- Not capturing last argument in a variable arg list in RHEL 7 [CB-31219]
- Proxy setting in sensorsettings.ini will not work with custom TLS certificate. [CB-30175]
- Unloading the cbsensor module can cause some programs to exit due to an unexpected return from a socket read. [CB-26764]

- Sometimes user is reported as unknown with eBPF sensor [CB-28017]
- Holding the process tracking table spin lock for too long [CB-31312]

Known Issues and Limitations

Known issues associated with this sensor version:

- IP addresses are not supported as SAN entries in a custom certificate
- Sensor accepts expired certificates in strict mode, but will close connections when using an expired certificate. [CB-30424]
- Error message on eBPF sensors upon upgrade to 7.0.0: cbdaemon.service: Failed at step EXEC spawning No such file or directory
- 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]
- ICMP traffic is allowed when a sensor is isolated. [CB-6623]
- 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.