



## Introduction

---

This document provides change information regarding CB Protection v7.4.6.80 Linux agents and instructions for installation.

## Installation

You can upgrade CB Protection Linux Agents without having to upgrade their CB Protection Server. Please visit the latest *CB Protection User Guide* for more information.

For information regarding what Linux operating systems are supported in this release, please review the [CB Response sensors & CB Protection agents](#) document on the Carbon Black User Exchange.

## Purpose of This Release

The CB Protection v7.4.6.80 Linux Agent is primarily a maintenance release.

For more detailed information, please review the specific sections carefully:

- [New Features and Product Enhancements](#)
- [Corrective Content](#)
- [Known Issues and Limitations](#)

## New Features and Product Enhancements

In this release, we have included several new enhancements to ensure that our product is prepared to keep you and your endpoints secure. These changes include:

- Support for RHEL 8.2
- Memory leak reductions
- Improved allocation of large Kernel memory blocks

# Carbon Black.

## Corrective Content

This section lists defects fixed in this release, CB Protection 7.4.6.80 Linux Agent.

Item #	Description
EP-10262	Fixed an issue where Linux agent upgrades from version to 7.4.4 to 7.4.6 intermittently displayed an error on the console indicating that the process has stopped.  Note: This issue still exists if upgrading from 7.4.2 to 7.4.4.
EP-10832	Fixed an issue where an “unsupported kernel version installed” message displayed in the health check and on Errors.bt9 file.
EP-10735 EP-10736 EA-16102	Fixed several issues affecting memory usage and kernel allocation that will have a positive impact on product performance and reliability

## Known Issues and Limitations

The following table lists the known issues and limitations present in the CB Protection 7.4.6.80 Linux Agent.

Item #	Description
NA	Prelinking must be disabled on Red Hat and CentOS computers before installing agents. When prelinking is enabled, executable file content will be changed whenever prelinking runs, which will bloat server inventory and result in many more files that need to be approved. This makes it difficult to ascertain whether an executable file was maliciously modified since each instance can have a unique hash.
NA	If you have an existing CB Response Sensor running on your system and you wish to install the CB Protection Agent, a reboot will be required after the installation is completed.

# Carbon Black.

Item #	Description
NA	There is a new CB Response Updater available for Linux systems that are running both CB Protection Agents and CB Response Sensors. This updater can be enabled from the CB Protection console on the <b>Rules &gt; Software Rules &gt; Updaters</b> tab. Be sure to also enable the updater for Redhat Software Update.
NA	Reboot of an endpoint containing both CB Protection Agent v7.4.2 and CB Response Sensor may take several minutes.
EP-201	If a file is renamed with symlink, the event that reports this action shows an empty filename (quotation marks with nothing between them).
EP-344	<p>On some Linux systems, the CB Protection Agent notifier might not start automatically after installation or upgrade.</p> <p>There are several ways to remedy this:</p> <ul style="list-style-type: none"> <li>• The notifier can be started manually with root privileges. From the location <code>/opt/bit9/bin</code>, run the command: <b><code>./daemonize_notifier.sh</code></b></li> <li>• You can reboot the endpoint and the CB Protection Agent notifier should start automatically.</li> <li>• You can log out and log back in. However, this will not work with an SSH session running with the <code>-X</code> or <code>-Y</code> option. In that case, if you want to use the notifier, start it using one of the previous methods.</li> </ul>
EP-850	<p>If a system is stressed, it is possible for the OOM Killer to kill the <code>b9daemon</code> process. It is recommended that you exempt the <code>b9daemon</code> process from the OOM Killer as it cannot currently be blocked via tamper protection. The exemption can be created running the following command as the root user: <b><code>echo -1000 &gt; /proc/`pgrep b9daemon`/oom_score</code></b></p> <p>This command could be run as a chron job on a regular basis (e.g., once an hour). To verify if OOM has killed the <code>b9daemon</code>, the <code>syslog</code> can be checked as follows: <b><code>grep -i kill /var/log/messages</code></b></p> <p>If the OOM Killer terminated a process, the command would show results similar to this: <b><code>host kernel: Out of Memory: Killed process 1402 (b9daemon)</code></b></p> <p><b>Note:</b> While <code>oom_adj</code> can be used, this has been deprecated in RH6/7; the current recommendation for RH6/7 is to use <code>oom_score</code> file.</p>

# Carbon Black.

Item #	Description
EP-2817	Incorrect logic could intermittently allow the agent to misclassify a mount as a local drive if the mount point is ever lost or disconnected. This issue can be worked around by unmounting and remounting.
EP-3392	If the b9daemon is stopped via b9cli -shutdown and then restarted via b9cli -startup, the notifier is not automatically started. To manually start the notifier run the shell script <b>daemonize_notifier.sh</b> located under /opt/bit9/bin.
EP-7786	A Debug Level error, <i>Error (1)</i> ..., displays on the Linux agent after you send the debug level from the server to that agent.
EP-7903	Despite creating a custom rule for a trusted path that would allow and promote the files within that folder, the file state does not change after execution from that trusted folder.
EP-8203	Running a Baseline Drift Report produces no results for Linux agents.
EP-8349	Linux Agent upgrade fails if Linux Agent is running.
EP-8834	On the server events page, names associated with rules created for Linux triggering an execution block event may not display in the "Rule Name" Column.
EP-8845	Custom Rules using the macro, <OnlyIf>, do not work. For example, the macro, <OnlyIf:ConnectedToServer:No>, behaves the same regardless of connection status.
EP-8885	ELF files are not recognized as installer files.
EP-8912	On the server "Computer Details" page, the Debug Level may display the incorrect set level for Linux agents.
EP-8923	On the server events page, Tamper Protection warning events do not include "From" Locations on Linux agents.
EP-8932	The time in which a Policy Override code expires may not be communicated correctly depending on the Client/Server time zone. <b>NOTE:</b> This issue was resolved with CB Protection Server 8.1.8; however, if you have not upgraded to 8.1.8, the issue persists.
EP-8950	Custom rules using a process pattern including a prepended wildcard, such as " <i>*folder</i> " do not block files as expected.
EP-9022	After modifying the "Notifier Text" when editing the enforcement policy advanced settings for blocking scripts, the resulting error that occurs when triggering the notifier does not display in the log.

# Carbon Black.

Item #	Description
EP-9030	After restoring server from backup, an Alert erroneously displays regarding the Linux agent: "Host Package Not Found".
EP-9434	Repeated, unclean, shutdowns can result in a cache that grows exponentially and thus negatively impacts agent and device performance.
EP-9556	When upgrading from 7.4.2 to 7.4.4 on Oracle Linux 8.0, the upgrade may fail. In order to workaround this issue you must use a special set of commands that can be found in this <a href="#">KB article</a>
EP-10262	When upgrading a Linux agent specifically from version 7.4.2.112 to 7.4.4, an error may display on the console indicating that the process has stopped. <b>Note:</b> This error has been resolved when upgrading from 7.4.4 to 7.4.6.
EP-10508	Occasionally, when copying one interesting file over another interesting file, the latter is no longer found by dascli/b9cli command.
44496	The process command line field in CB Protection events will list only the name of the executable that ran, not the arguments that were used to invoke that executable.
46389	You cannot add a custom notifier icon for Linux agents in this release.
49579	Some virtual machines running on VMWare Fusion may hang on reboot. Removing "rhgb quiet" from the kernel menu entry appears to work around this issue.

# Carbon Black.

## Contacting Carbon Black Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

<https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/ta-p/34324>

For your convenience, support for CB Protection is available through several channels:

Technical Support Contact Options
Web: <a href="#">User eXchange</a>
E-mail: <a href="mailto:support@carbonblack.com">support@carbonblack.com</a>
Phone: 877.248.9098

## Reporting Problems

When you call or email technical support, please provide the following information to the support representative:

Required Information	Description
<b>Contact</b>	Your name, company name, telephone number, and e-mail address
<b>Product version</b>	Product name (for example, CB Protection Server or Agent) and version number
<b>Hardware configuration</b>	Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
<b>Problem</b>	Action causing the problem, error message returned, and event log output (as appropriate)
<b>Problem severity</b>	Critical, Major, Minor, Request