CB PROTECTION

Release Notes: 7.4.4 Linux Agent

May 2020

Introduction

This document provides change information regarding CB Protection v7.4.4.109 Linux agents and instructions for installation.

Installation

As of the 8.1.4 server release, the Linux Agent no longer comes bundled with the CB Protection Server, nor does it require manual (command line) steps to add it to the server. 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 v7.4.4 (7.4.4.109) Linux Agent includes support for RHEL 8.1 and CentOS 7.7. As always, there was a focus on improved security, user interface fixes, and reliability. Changes include:

- Support for RHEL 7.8
- Support for RHEL 8.1
- Support for CentOS 7.7
- Ability to reject applications not running latest version of 1.2 TLS
- Numerous other improvements and bug fixes to increase security and usability.

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

Product security is our top priority for CB Protection. 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:

- Added ability for Linux agent to reject applications not using the latest 1.2 version of TLS.
    - You can choose whether or not the agent accepts TLS versions other than 1.2 through a configuration property.
    - You are notified when an application not using TLS 1.2 is executed when the property is enabled.
    - You receive no notifications when this property is disabled.
- Improved security by removing the CLI <copycache> command to remove user ability to gain access to content using the cache.

  Running the command <copycache> in the agent CLI will not work
- Improved event logging to capture all changes to enforcement policies.

  When an enforcement policy is changed, an entry displays in the log with the subtype: “Agent policy changed”.

  The agent log displays consumption of the changed policy.

Corrective Content

This section lists defects fixed in this release, CB Protection 7.4.4.109 Linux Agent.

Item #	Description
EP-6021	When pushing updates automatically from the CB Protection console, its use of BSX files removes the record of a CB Protection agent install from the RPM catalog.
EP-7509	Fixed issue where “Bit9” displayed in several locations within the notifier. Now, “Cb Protec*tion”* displays within the notifier Vendor and Description fields.
EP-8911	Fixed issue where RHEL 8 computers displayed the operating system “Redhat 7” on the computers page. Now, RHEL 8 computers correctly display Redhat 8 as the operating system.
EP-9122	Fixed issue where the index was not checked after a de-serialized string was terminated. Now, if a de-serialized string is terminated or if an error corrupts the bytes, by any means, which store length, the index is checked.
EP-9227	Fixed issue where the connection status on the Computer Details page did not update the icon to yellow when upgrading the agent. Now, the icon turns yellow during the upgrade, as expected.
EP-10171	Fixed reliability issue by improving cbproxy kernels so they always recompiled. Affected kernels are: RedHat/CentOS 7.6: 3.10.0-957.el7.x86_64 and all -957.x.y variants RedHat/CentOS 7.7: 3.10.0-1062.el7.x86_64 and all -1062.x.y variants [if any]

Known Issues and Limitations

The following table lists the known issues and limitations present in the CB Protection 7.4.4.109 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.
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 **Rules > Software Rules > Updaters** 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	On some Linux systems, the CB Protection Agent notifier might not start automatically after installation or upgrade. There are several ways to remedy this: • The notifier can be started manually with root privileges. From the location /opt/bit9/bin, run the command: **./daemonize_notifier.sh** • You can reboot the endpoint and the CB Protection Agent notifier should start automatically. • You can log out and log back in. However, this will not work with an SSH session running with the -X or -Y option. In that case, if you want to use the notifier, start it using one of the previous methods.

Item #	Description
EP-850	If a system is stressed, it is possible for the OOM Killer to kill the b9daemon process. It is recommended that you exempt the b9daemon 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: **echo -1000 > /proc/`pgrep b9daemon`/oom_score** 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 b9daemon, the syslog can be checked as follows: **grep -i kill /var/log/messages** If the OOM Killer terminated a process, the command would show results similar to this: **host kernel: Out of Memory: Killed process 1402 (b9daemon)** **Note:** While oom_adj can be used, this has been deprecated in RH6/7; the current recommendation for RH6/7 is to use oom_score file.
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 **daemonize_notifier.sh** located under /opt/bit9/bin.
EP-7786	A Debug Level error, *Error (1)*…,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-7906	CIFS connections are not supported with FIPS mode due to MD5 usage.
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.

Item #	Description
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.
EP-8950	Custom rules using a process pattern including a prepended wildcard, such as “*\folder” 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.
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-10262	When upgrading a Linux agent from version 7.4.2.112 to 7.4.4, an error may display on the console indicating that the process has stopped.
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 KB article
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.

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: User eXchange
E-mail: support@carbonblack.com
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
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (for example, CB Protection Server or Agent) and version number
Hardware configuration	Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, Major, Minor, Request