CB PROTECTION

Release Notes: Linux Agent 7.4.0

May 2019

Introduction

This document provides information for users installing CB Protection v7.4.0.25 Linux agents.

Installation

This v7.4.0 Linux agent no longer requires manual installation; however, you will need to have CB Protection Sever 8.1.4 or above. Please visit the CB Protection Server 8.1.4 User Guide for more information about installing and upgrading agents under this new process.

Once these files are installed, they may be used to deploy agents on Linux systems. Please review the *CB Response sensors & CB Protection agents: Linux* document on the Carbon Black User Exchange to determine the Linux operating systems that are supported in this release.

Purpose of This Release

This 7.4.0 agent release adds the following new features:

- FIPS 140-2 Support
- Support for Type-1 Hypervisors (PVM)

For more detailed information about these new additions and other improvements, please review the "What's New in 7.4.0?" section.

***Note**: This release also includes a security fix that may impact your environments. Please review the "**Corrective Content**" section for more information about this.*

Carbon Black, Inc. | 1100 Winter Street, Waltham, MA 02451 USA | Tel: 617.393.7400

What's New in This Release?

FIPS 140-2 Certification

FIPS 140-2 certification allows CB Protection to be deployed by federal agencies, including contracted service providers and other organizations requiring stringent security standards to protect sensitive information. This release adds support for FIPS compliant use with our Server and Linux agent.

Para-virtualization Support

Para-virtualization allows CB Protection to be deployed in environments utilizing XenServer. This Type 1 Hypervisor allows organizations to scale their IT Infrastructure rapidly and with fewer resources. This release adds support for Linux agents to be deployed on virtualized machines (domU) connected to Type 1 Hypervisors (dom0).

Corrective Content

Corrective Content in CB Protection 7.4.0 Linux Agent (Build .25)

- Fixed an issue where dmesg would display “system setup failed” in the “cbproxy loading” section when upgrading the agent. [EP-7686]
- Fixed an issue where an unapproved binary could be executed by exploiting the proc filesystem (procfs). This includes files that are banned in the Protection console. For more information about this bypass and resolution please visit this Security Bulletin from our Product Security Team. [EP-7391]
- CB Protection agent no longer allows for per-agent CLI passwords by default. [EP-7742]

Known Issues and Limitations

This section lists known issues and limitations of this Linux agent release. See also the *Known Issues and Limitation*s section in the separate Release Notes for your CB Protection Server version for issues that might be relevant to this v7.4.0 Linux agent release.

- 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.
- 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.
- 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-3392]
- 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-2817]
- If the /srv/bit9 directory is a separate mount point (not the root file system), you may see the following spurious warning when uninstalling the agent:
  Warning: directory /srv/bit9: remove failed: Device or resource busy.
  The agent will correctly be uninstalled, leaving the /srv/bit9 mount point intact. [EP-2577]
- If you wish to install the CB Response Sensor on a system running the CB Protection Agent at High, Medium, or Low Enforcement, put the CB Protection Agent into Local Approval to successfully complete the installation of the CB Response Sensor. Be sure to restore the endpoint to its previous Enforcement Level after sensor installation is complete. [EP-313]
- Reboot of an endpoint containing both CB Protection Agent v7.4.0 and CB Response Sensor may take several minutes.
- 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.

- 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-850]
- On some Linux systems, the CB Protection Agent notifier might not start automatically after installation or upgrade. [EP-344, EP-359]

  There are several ways to remedy this:

  1. The notifier can be started manually with root privileges. From the location **/opt/bit9/bin** run the command:

     ```
     ./daemonize_notifier.sh
     ```
  2. You can reboot the endpoint and the CB Protection Agent notifier should start automatically.
  3. 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.
- When a system has synchronous and asynchronous write file operations, the Linux agent could miss some file writes. This is related to EXT4 but may extend to other file systems. [EP-131]
- If a file is renamed with symlink, the event that reports this action shows an empty filename (quotation marks with nothing between them). [EP-201]
- 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. [49579]
- 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. [44496]
- You cannot add a custom notifier icon for Linux agents in this release. [46389]
- When pushing updates automatically from the CB Protection console, its use of BSX files will remove the record of a CB Protection agent install from the RPM catalog. [EP-6021]
- CIFS connections are not supported with FIPS mode due to MD5 usage. [EP-7906]

Contacting Carbon Black Support

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

- **Web:** User Exchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (CB Protection server and agent version)
- **Hardware configuration:** Hardware configuration of the CB Protection 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