Carbon Black.

Summary

CB Response 6.4.0 is a feature release of the CB Response server and console. The 6.4.0 release contains new features such as TLS Certificate Management and a Query Duration widget, in addition to bug fixes and Python 3 and third-party dependency updates.

These release notes include the following information:

This release includes the following components:

- Server version 6.4.0.190610
  Release Notes: (this document)
- Windows Sensor version 6.2.2.190503
  Release Notes
- MacOS Sensor version 6.2.5.190604
  Release Notes
- Linux Sensor version 6.1.10.10169
  Release Notes

Each release of CB Response software is cumulative and includes changes and fixes from all previous releases.

TLS Certificate Management [CB-16210]

6.4.0 server includes the new TLS Certificate Management feature. CB Response Servers can push SSL certificates to sensors, thereby making sensor management easily manageable and flexible.

This feature includes the following abilities:

- Provide certificates that are signed by the user's organization.
- Uses different server certificates to authenticate connections between the CB Response Server and various sensor groups. This reduces the exposure to a compromised server certificate.
- Adds stricter validation methods to certificate pinning, so that if a server certificate that is used by a sensor has expired or fails to meet other operating-system-specific criteria, server-sensor communication is disabled.

See the *CB Response* *6.4.0 User Guide* for detailed feature description.

CB Response Server can still use the standard certificate validation method that was available in previous server versions. Past and current sensors continue to support this method.

Query Duration Widget [CB-19650]

6.4.0 server has a widget that displays the 50 slowest running queries. This widget can help users write more efficient queries by making Process Search performance visible. This feature is available for Global admins only. See the *CB Response* *6.4.0 User Guide* for more information.

Update Third-party Dependencies [CB-22416]

Third-party dependencies are updated so that there are no outstanding vulnerabilities. The following packages are updated in 6.4.0 server:

- Rabbit MQ 3.7
- ANTL 4
- Apache FileUpload 1.3.3
- Python 3 dependencies

All packages will be automatically updated upon server upgrade.

Document Contents

This document provides information for users who are upgrading to CB Response Server version 6.4.0 from previous versions, as well as for users who are new to CB Response. The key information that is specific to this release is provided in the following major sections:

- **Preparing for Server Installation or Upgrade** – Describes requirements and key information that is needed before beginning the installation process for the CB Response server.
- **New Features** – Provides a quick reference to the new and modified features that are introduced with this version.
- **Corrective Content** – Describes issues that are resolved by this release, as well as more general improvements in performance or behavior.
- **Known Issues and Limitations** – Describes known issues or anomalies in this version.

Additional Documentation

This document supplements other Carbon Black documentation. Click here to search the full library of CB Response user documentation on the Carbon Black User Exchange.

Technical Support

CB Response server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that might develop during the installation or upgrade process. Our Professional Services organization is also available to help ensure a smooth and efficient upgrade or installation.

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

Reporting Problems

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 Response server and sensor version).
- **Hardware configuration:** Hardware configuration of the CB Response server (processor, memory, and RAM).
- **Document version:** For documentation issues, specify the version and/or date of the manual or document that you are using.
- **Problem:** Action causing the problem, the error message returned, and event log output (as appropriate).
- **Problem severity:** Critical, serious, minor, or enhancement request.

Note: Before performing an upgrade, Carbon Black recommends reviewing content on the User Exchange for the latest information that supplements this document.

[On-Prem Only] Preparing for Server Installation or Upgrade

This section describes the requirements and key information that is needed before beginning the installation process for the CB Response server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. Next, see the appropriate section of the *CB Response Server/Cluster 6.4.0 Management Guide* for specific installation instructions for your situation:

- **To install a new CB Response server**, see "Installing the CB Response Server".
- **To upgrade an existing CB Response server**, see "Upgrading the CB Response Server".

Yum URLs

CB Response Server software packages are maintained at the Carbon Black yum repository (yum.distro.carbonblack.io). **The links will not work until the on-prem GA date**.

Our yum links for the CB Response server have changed. The following links use variables to ensure that you install the correct version of CB Response, based on your machine's OS version and architecture.

Use caution when pointing to the yum repository. Different versions of the product are available on different branches as follows:

- **Specific version:** The 6.4.0 version is available from the Carbon Black yum repository specified in the following base URL:

  baseurl=https://yum.distro.carbonblack.io/enterprise/6.4.0-2/$releasever/$basearch

  This link is available as long as this specific release is available. It can be used even after later versions have been released, and it can be useful if you want to add servers to your environment while maintaining this version.

- **Latest version:** The latest supported version of the CB Response server is available from the Carbon Black yum repository specified in the following base URL:

  baseurl= https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/

  This will point to version 6.4.0-1 until a newer release becomes available, at which point it will automatically point to the newer release.

Note: Communication with this repository is over HTTPS and requires the presence of appropriate SSL keys and certificates. During the CB Response server install or upgrade process, other core CentOS packages can be installed to meet various dependencies. The standard mode of operation for the yum package manager in CentOS is to first retrieve a list of available mirror servers from http://mirror.centos.org:80 and then select one of those mirrors to download the actual dependency packages. If your CB Response server is installed behind a firewall, it is the responsibility of the local network and system administrators to ensure that the host machine can communicate with standard CentOS yum repositories.

[On-Prem Only] System Requirements

Operating system support for the server and sensors is listed here for your convenience. The *CB Response Operating Environment Requirements* document describes the full hardware and software platform requirements for the CB Response server and provides the current requirements for systems that are running the sensor.

Both upgrade and new customers must meet all of the requirements specified here and in the CB Response Operating Environment Requirements document before proceeding.

Server / Console Operating Systems

Note: For best performance, Carbon Black recommends running the latest supported software versions.

- CentOS 6.7-6.10 (64-bit)
- CentOS 7.3-7.6 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3-7.6 (64-bit)

Installation and testing are performed on default install using the minimal distribution and the distribution's official package repositories. Customized Linux installations must be individually evaluated.

Sensor Operating Systems (for Endpoints and Servers)

For the current list of supported operating systems for CB Response sensors, see https://community.carbonblack.com/docs/DOC-7991.

Note: Non-RHEL/CentOS distributions or modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.

Configure Sensor Updates Before Upgrading Server

CB Response 6.4.0 comes with updated sensor versions. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups instead of all at once.

Decide if you would like the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid impact on network and server performance. To avoid inadvertently upgrading all sensors at the same time, Carbon Black also strongly recommends that you review your Sensor Group Upgrade Policies before upgrading your server. For detailed information on the Sensor Group Upgrade Policy, see the Sensor Group section of the *CB Response 6.4.0 User Guide*.

To configure the deployment of new sensors via the CB Response web UI, follow the instructions in the *CB Response 6.4.0 User Guide*.

Corrective Content

1. Sensors show the correct status in the UI (installed/uninstalled) when a sensor is uninstalled and reinstalled with the same install package and when the global VDI setting is enabled in cb.conf. [CB-14283]

2. Leading forward '/' and Backslash '\' has been tokenized in the Process Analyse page. Command line hyperlink that has queries that begin with leading forward '/' and backslash '\' will return expected search results. [CB-25072][CB-19124]

3. Sometimes a Solr core has a missing or corrupt cb.core.conf file. This causes a disruption during the core rollover. The rollover process relies on the configuration file. This fix makes sure that the file exists if it was deleted, corrupted or not created initially. [CB-21670]

4. Process search with multiple instances that have the same process name was returning inaccurate results in the preview. With this fix, each preview is distinct and matches the entry that was clicked. [CB-21914][CB-22552]

5. Search results from range queries with nested negations will work as expected. [CB-20269]

6. The sensors versions filter has been fixed to reflect only sensor versions in the results on the Sensor Page. [CB-24254]

7. When switching between watchlists, Results no longer display stale search results until the currently searched watchlist query completes the run. [CB-18183]

8. Updating a watchlist query with an encoded character does not delete the watchlist. [CB-25653]

9. When generating diagnostics from the master node, the `\cb_services\coreservices\sensor_report_summary and sensor_report` will return as expected. [CB-23746]

10. On the Process search page, if the search bar is empty, “q=” will no longer be sent to SOLR. Users have to click on the “Search” button to run a query. [CB-17983]

Known Issues

1. RabbitMQ for minions may not start at once during the server upgrade. Repeat service restart attempts will get the minions to restart. [CB-27512]

2. Invalid query when creating a watchlist from a Threat Feed. When creating a watchlist from a Threat Feed, CB Response incorrectly creates the query and the watchlist creates an error and does not run. To see if your watchlist has formed an error, check the Watchlist page for the status. As a workaround, the CB Response Team suggests clicking the **Search Binaries** or **Search Process** hyperlinks on the Threat Feed, and then selecting the **Add/Create Watchlist** action from the search page.

3. If the browser time zone is different from the server time zone, you might notice a discrepancy in the last check-in time shown for sensors. [CB-20076]

4. The CSV export of the user activity audit is malformed in certain cases. [CB-18936]

5. The CSV export of **Recently Observed Hosts** has no header row. [CB-18927]

6. When using a custom email server, the user cannot enable or disable Alliance Sharing. The workaround is to disable the custom email server, make the change, then re-enable the custom email server. [CB-20565]

7. For sensor upgrades to work properly, you might need to configure McAfee EPO to exclude `c:\windows\carbonblack\cb.exe` from its **Prevent creation of new executable files in the Windows folder** option. [CB-7061]