Release Notes: Server v6.5.2

November 2019

Summary

Important Notice: CB Response 6.5.2 has a fix for a major bug that was introduced in 6.5.0 and 6.5.1. In some cases, event data was incorrectly discarded and not ingested by CB Response Server. Because events were not ingested, the lost event data was not immediately apparent unless an integration, such as Event Forwarder, forwarded the data to another system. CB Response 6.5.2 fixes for this bug.

Please see UeX post for more information.

This release includes features and bug fixes that were included in 6.5.0 and 6.5.1 CB Response Server. The 6.5.2 release is compatible in FIPS hardened servers.

These release notes include the following information:

This release includes the following components:

- Server version 6.5.2.191108

  Release Notes: (this document)

- Windows Sensor version 6.2.4.190820
  Release Notes
- MacOS Sensor version 6.2.6.190912
  Release Notes
- Linux Sensor version 6.2.1.10119
  Release Notes

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

Document Contents

This document provides information for users who are upgrading to CB Response Server version 6.5 from previous versions, and for users who are new to CB Response. The key information specific to this release is provided in the following major sections:

- **Preparing for Server Installation or Upgrade** – Describes requirements to meet and information 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, and 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.

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

This section describes the requirements and key information that is needed before installing a CB Response server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. See the appropriate section of the *CB Response Server/Cluster Management Guide* 6.5 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 make use of variables to ensure that you install the correct version of CB Response, based on your machine's operating system 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 6.5 version is available from the Carbon Black yum repository that is specified in the following base URL:

  baseurl=https://yum.distro.carbonblack.io/enterprise/6.5.2-1/$releasever/$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 the same version.

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

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

  This URL will point to version 6.5.0-1 until a newer release becomes available, at which time 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 a mirror from which to download the dependency packages. If a CB Response server is installed behind a firewall, local network and system administrators must make sure 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. This document is available on the Carbon Black User Exchange.

Both upgrading 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 the following page in the Carbon Black User eXchange:

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 6.5 comes with updated sensor versions. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups.

Decide whether you want the new sensor to be deployed immediately to existing sensor installations, or install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid network and server performance impact. We strongly recommend that you review your sensor group upgrade policies before upgrading your server, to avoid inadvertently upgrading all sensors at the same time. For detailed information on Sensor Group Upgrade Policy, see the Sensor Group section of the *CB Response 6.5 User Guide*.

To configure the deployment of new sensors via the CB Response web console, follow the instructions in the *CB Response 6.5 User Guide*.

New Features

CB Response Server in FIPS Hardened mode

In this release, CB Response server is now compatible with RHEL servers operating in FIPS mode as described here: 10.2. Federal Information Processing Standard (FIPS) - Red Hat Customer Portal

Storage of passwords has been updated. The storage changes take effect for each user as they log in. In a future release (to be determined) inactive users will require a password reset before they can log in. The following are not affected:

- CB Cloud users
- On Prem SSO users
- Users created on a fresh install of 6.5
- Users created after an upgrade to 6.5

Online help for CB Response Server

CB Response User Guide is now available in the product. It can be accessed by clicking **Help > User Guide**. The in-product User Guide opens in a new tab. It works at any screen width, has a search capability, and internal links for easy navigation.

Size of an HTTP request

Two new variables are printed in access logs for each received row/request; for example, `bytes_sent` and `request_length`, which are bytes that are sent to the client (including header) and bytes received from a client in request (including header), respectively. [CB-14538]

Network Isolation exclusions

A new configuration setting for sensor groups lets you specify IP addresses and URLs that a sensor can access even when the endpoint is isolated. In previous versions, an isolated sensor could communicate with CB Response Server only, but there are cases where additional access is required (for example, to interact with VPNs, proxy servers, or other security products such as CB Protection). The new setting can be found in the **Settings** section of editing a sensor group.

Note

- Isolation exceptions are unique per group. Multiple groups can have some or all of the same exceptions, but they must be configured on a group-by-group basis.
- If you have permission to edit a group, you may edit isolation exceptions for a group.
- This feature is disabled by default, and does not appear on the **Group Settings** page unless it is enabled. To enable the feature, add `IsolationExclusionsEnabled=True` to `/etc/cb/cb.conf` and restart services.

See the *CB Response 6.5 User Guide* for more information.

Corrective Content

1. A defect was introduced in version 6.5.0 and version 6.5.1 that can result in a loss of endpoint event data. In some cases, events are not ingested by CB Response. This data is still available if CB Response is configured to export events via integration (such as the CB Event Forwarder), but the data is not stored in the CB Response event database. This defect is repaired in version 6.5.2 CB Response server. [CB-29153]

2. The search box in the Activity Audit page under **User Management** works as expected.[CB-22992]

3. To create watchlists with special characters like '&', the special character must be enclosed in single or double quotes. Quotes cannot be nested. This is especially important when creating watchlists from non-urlencoded search queries. [CB-23654]

4. Any queries that the **Add Criteria** dropdown in the Binary search page generates now creates valid watchlists. Previously broken watchlists will not be fixed automatically with this upgrade. You can regenerate the watchlists or manually fix them. [CB-27062]

5. Example logger configurations in the comments of the `logger.conf` files now have correct paths. [CB-20566]

6. `SolrTimePartitioningDailyStartTime` creates Solr partitions at the specified time. [CB-26511]

7. When a feed is disabled, it will not be picked up my `watchlist_search job_runner`. This fix eliminates additional load on the server. [CB-20515]

8. Removed lingering links to VirusTotal feed. [CB-16374], [CB-27468]

9. IP address is accurately formatted in the downloaded CSV from the Process Search page. [CB-15266]

10. There are two download links on the binary details page: one for frequency, and the other for observed hosts. Both links download accurate CSV files. [CB-18332]

11. Resolved an issue when using the nginx IP whitelist apply API endpoint on a cloud cluster. [CB-26868]

12. The issues with too many reserve calls, too much throttling and growing backlogs has been fixed. As a result, Ingestion will not be slow. [CB-27838]

13. Server will handle bad data sent from the sensor without stalling ingestion, instead of continuously retrying a bad sql insert. [CB-27447]

14. After updating a watchlist, alerts and email if subscribed will be generated as expected. [CB-27880]

15. In rare cases, a sensor registering under VDI could be assigned a new ID even if it had previously registered under an existing ID, due to a delay in loading registration data into

the datagrid component. If this ever re-occurs, the error will now be caught, properly logged, and the sensor will be signaled to try again later. [CB-28242]

16. For response cloud users, Duo two factor authentication will work for Global admin and users (non-global admin users). [CB-28104]
17. Alert widget on HUD will auto-update like all other widgets on the page.[CB-27813]
18. Binary Dwell and Hygiene HUD widgets will be limited to the last 30 days. The data represented in these graphs will not be squished. [CB-27835]
19. Alerts from a Windows host will be displayed on the right hand side panel of a CB LiveResponse Session. [CB-22993]
20. ‘feed_search’ overnight job is more lightweight. The feed_search job that runs overnight was too heavy, and took down the server for a brief period of time, triggering alerts.[CB-26483]
21. 'Status' column sorting is applied to all tabbed pages on the Sensor List page.[CB-15448]
22. When a new server certificates (Settings / Server Certificates) is added, the user must specify two SAN DNS entries, but they cannot include any wildcard characters such as "*". This use case was not validated. This has been fixed: new server certificates are now validated to ensure that both SAN DNS names do not contain wildcards, and will not be accepted until this validation passes. [CB-28480]
23. If a feed's report is deleted (i.e., removed from feed report json) and we perform full sync on feed. The corresponding watchlist will now be removed.[CB-28082]

Known Issues

1. After an upgrade of Server and Sensor, older files did not get SHA-256 values. When an older file is executed, it creates a process event which contains SHA-256. When a user clicks on the link, the binary store shows no SHA-256.[CB-24519]
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 does not run and creates an error. To see if your watchlist that was created from a threat feed that formed an error, check the status on the Watchlist page. As a workaround, the CB Response Team suggests clicking the **Search Binaries** or **Search Process** hyperlinks on the Threat Feed, and then using the **Add/Create Watchlist** action from the Search page.
3. If the browser timezone is different from the server timezone, you might notice a discrepancy in the last sensor check-in time. [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, you 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]

Contacting Support

CB Response server and sensor update releases are covered under the Carbon Black Customer Maintenance Agreement. Technical Support can assist with any issues that might develop. 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 versions)
- **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 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 that you review the content on the User Exchange.