Release Notes: Server 7.5.0

June 2021

Summary

VMware Carbon Black EDR 7.5.0 is a feature release of the VMware Carbon Black EDR (formerly CB Response) server and console. This release delivers improvements to sensor service performance, improvements to the Process Search and Process Analysis pages, support of SELinux “enforcing mode”, integration of the Airgap Feed and Yara Manager into EDR Server, and various small-scale enhancements and bug fixes. Also, this release is expected to achieve Common Criteria certification, which is currently in “Evaluation” with National Information Assurance Partnership (NIAP).

See the New Features and Corrective Content sections for more details.

This release notes document includes the following sections:

This release includes the following components:

- Server version 7.5.0.210527
  Release Notes (this document)
- Windows Sensor version 7.2.0.17354
  Release Notes
- MacOS Sensor version 7.1.1.16418
  Release Notes
- Linux Sensor version 7.0.3.15300
  Release Notes

Each release of VMware Carbon Black EDR software is cumulative and includes changes and fixes from all previous releases.

Document Contents

This document provides information for users who are upgrading to VMware Carbon Black EDR Server version 7.5.0 from previous versions, and for users who are new to VMware Carbon Black EDR and are installing it for the first time.

The key information specific to this release is provided in the following major sections:

- **[On-Prem Only] Preparing for Server Installation or Upgrade** – Describes requirements to meet and information needed before beginning the installation process for the VMware Carbon Black EDR server.
- **Configure Sensor Update Settings Before Upgrading Server** –
- **New Features** – Provides a quick reference to new and modified features that are introduced in this version.
- **Corrective Content** – Describes issues that are resolved by this release, and general improvements in performance or behavior.
- **Third Party Software Updates** – Describes updates of third party software included in this version.
- **Known Issues** – Describes known issues or anomalies in this version.
- **Contacting Support** – Describes ways to contact Carbon Black Technical Support and what information to have ready.

Additional Documentation

This document supplements other Carbon Black documentation. Supplemental release documentation can be found in the new Carbon Black EDR section of docs.vmware.com, rather than on the VMware Carbon Black User Exchange, where release documentation used to be published.

In addition to this document, you should have access to the following key documentation for VMware Carbon Black EDR Server 7.5.0:

- *VMware Carbon Black EDR 7.5 User Guide:* Describes how to use the Carbon Black EDR servers that collect information from endpoint sensors and correlate endpoint data with threat intelligence.
- *VMware Carbon Black EDR 7.5 Server / Cluster Management Guide:* Describes installation, configuration, and upgrade of Carbon Black EDR servers.
- *VMware Carbon Black EDR 7.5 Unified View Guide:* Describes the installation and use of the VMware Carbon Black EDR Unified View server. Information on server hardware sizing requirements and software platform support is included.

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

This section describes the requirements and key information that is needed before installing a VMware Carbon Black EDR server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. See the appropriate section of the *VMware Carbon Black EDR 7.5 Server/Cluster Management Guide* for specific installation instructions for your situation:

- **To install a new VMware Carbon Black EDR server**, see “Installing the VMware Carbon Black EDR Server”.
- **To upgrade an existing VMware Carbon Black EDR server**, see “Upgrading the VMware Carbon Black EDR Server”.

Customers on Server 5.x, please note:

Direct upgrades from Server 5.x to Server 7.x *are not* supported. Please refer to Page 31 of the *VMware Carbon Black EDR 7.5 Server/Cluster Management Guide* and this VMware Carbon Black User Exchange announcement for more information.

Yum URLs

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

The following links use variables to make sure you install the correct version of VMware Carbon Black EDR, 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 7.5.0 version is available from the Carbon Black yum repository, that is specified in the following base URL:

  baseurl= https://yum.distro.carbonblack.io/enterprise/7.5.0-1/$releasever/$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 VMware Carbon Black EDR 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 7.5.0-1 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 appropriate SSL keys and certificates. During the VMware Carbon Black EDR 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 VMware Carbon Black EDR 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 *VMware Carbon Black EDR 7.5 Operating Environment Requirements* document describes the full hardware and software platform requirements for the VMware Carbon Black EDR server and provides the current requirements and recommendations for systems that are running the sensor.

Both upgrading and new customers must meet all of the requirements specified here and in the *VMware Carbon Black EDR 7.5 Operating Environment Requirements* document before proceeding.

Server / Console Operating Systems

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

- CentOS 6.7 - 6.10 (64-bit)
- CentOS 7.3 - 7.9 (64-bit)
- CentOS 8.1 - 8.3 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7 - 6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3 - 7.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.1 - 8.3 (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.

However, if the customers are pinning dependencies to a specific OS version, the product only supports the following software versions for the Carbon Black EDR Server and Unified View:

- CentOS 6.7 - 6.10 (64-bit)
- CentOS 7.5 - 7.9 (64-bit)
- CentOS 8.2 - 8.3 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7 - 6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.5 - 7.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.2 - 8.3 (64-bit)

Note: Versions 7.3, 7.4, and 8.1 (64-bit) of CentOS/RHEL are not supported if customers are pinning dependencies.

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 VMware Carbon Black EDR 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 Update Settings Before Upgrading Server

VMware Carbon Black EDR 7.5.0 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 *VMware Carbon Black EDR 7.5 User Guide*.

To configure the deployment of new sensors via the VMware Carbon Black EDR web console, follow the instructions in the *VMware Carbon Black EDR 7.5 User Guide*.

New Features

Common Criteria Certification

VMware Carbon Black EDR 7.5.0 is *expected* to achieve Common Criteria certification, an international set of guidelines and specifications developed for the evaluation of information security products, specifically to ensure they meet an agreed-upon security standard for government deployments. VMware Carbon Black EDR 7.5.0 entered into an “Evaluation” status with National Information Assurance Partnership (NIAP) in February 2021.

Sensor Service Performance Improvements

VMware Carbon Black EDR 7.5.0 introduces a re-architecture of the way in which sensors check in to the server. The result is a significant improvement in sensor check-in rates and overall system performance and stability.

Process Analysis Page Improvements

VMware Carbon Black EDR 7.5.0 introduces a re-architecture of the Process Analysis page that results in faster loading times and the ability to filter across all events in the process. Process results now load incrementally, rather than waiting to load and populate all at once, so you are able to begin your investigations faster and avoid time-outs more consistently. Also, we have resolved the limitation of only being able to filter process results on the current page: you can now filter across all events of the process and the filters display the total number of matching results across the full lifetime of the process*, rather than only the number of matching results on the current page.

Here are some additional specific improvements:

- Visibility into the full history of the process in the Event Timeline view
- A purple triangle indicates the “Current position” within the Event Timeline view
- An orange triangle indicates the process segment you selected on the Process Search page (as before). It is now labeled as the “Starting position” of the process within the Event Timeline view.

Please note: Checks for suppression of child processes (childprocs) are now performed upon expansion of an individual event, rather than being completed automatically for all displayed events. The ‘Suppressed’ field within Process Metadata will have a status of “Checking…” until the check returns a value of “Yes” or “No” or times-out with a status of “Timed out while checking”. Time-out duration is configurable via *cb.conf*.

*In the vertical Filters pane, the number of matching results will display for each facet if the processing time does not exceed the specified time-out value. If the processing time *does* exceed the time-out value, the following message will appear, “Showing partial results without facet counts. Decrease timeline window size to avoid timeout.” This time-out duration is also configurable in *cb.conf*, so the time-out value can be increased and/or the Event Timeline window size can be reduced to attain filter facets with populated prevalence counts.

Please see the Process Search and Analysis section of the *VMware Carbon Black EDR 7.5 User Guide* for more details.

Process Search Page Improvements

VMware Carbon Black EDR 7.5.0 introduces several small-scale enhancements to the Process Search page:

- The Process Search bar can now be expanded to show the entire query by clicking and dragging from the bottom right of the text box.
- The Process Search Query helper did not include the “terminated” field in previous versions. A query that included “terminated:true” or “terminated:false” would result in a

syntax error. The “terminated” field has been added in Server 7.5.0 as an ‘Available Criteria’ within the ‘Primary’ Category of the ‘ADD SEARCH TERMS’ query builder, mitigating the error.

- The Process Search ‘ADD SEARCH TERMS’ query builder has much improved error handling and can now display more relevant validation error messages.
- In the ‘ADD SEARCH TERMS’ query builder, the Bulk IOC "Is not" selection now parses entries into the correct syntax.
- "All time" is switched to "All available" in the timeframe selection dropdown menu to the right of the search bar to more accurately reflect that results are based on retention.
- “Last 24 hours” has been added as an option in the timeframe selection drop-down menu to the right of the search bar.
- The 12-hour clock has been updated to a 24-hour clock so the time format is consistent across the Process Search and Process Analysis pages.

Please see the Process Search and Analysis section of the *VMware Carbon Black EDR 7.5 User Guide* for more details.

SELinux Enforcing Mode

VMware Carbon Black EDR 7.5.0 has been validated to work with SELinux “enforcing mode” (default), without additional hardening rules.

Airgap Feed (cb-airgap-feed) in EDR Server

Beginning with VMware Carbon Black EDR 7.5.0, the cb-airgap-feed script is incorporated into the EDR distribution as an internal tool. The Airgap utility continues to work the same way, using the same command line options. It is located at /usr/share/cb/cbfeed_airgap. The usage and command line options are the same, except that we have added a -v option for verbose logging and it logs to /var/log/cb/cli/cli.log, following the same pattern used in other EDR CLI utilities. For more information, please see the *VMware Carbon Black EDR 7.5 User Guide* and *Carbon Black EDR Airgap Feed*.

Yara Manager in EDR Server

Beginning with VMware Carbon Black EDR 7.5.0, the Yara Manager is incorporated into the EDR Server user interface for authentication. Please refer to the *VMware Carbon Black EDR 7.5 User Guide* and *CB Yara Manager guide for EDR* for specific information on configuring, authenticating, and operating the Yara Manager.

Visibility into Custom Threat Report Errors

VMware Carbon Black EDR 7.5.0 introduces visibility into rejected custom Threat Reports and why a report was rejected, so that customers who added a custom Threat Intelligence Feed

know which Threat Report(s) within that feed (if any) are rejected (and therefore inactive) and why. The customer can then try to correct their custom Threat Intelligence Feed.

Previously, the only indications of a Threat Report validation failure were error messages in the enterprise debug log. These failures were otherwise silent, and the user did not necessarily notice that they had one or more missing or defective reports. Starting in EDR Server 7.5.0, validation errors for custom Threat Reports are displayed as *FeedSynchronizer* Task or *feed_sync* Job errors in the Task Errors widget in the Heads Up Display (HUD), and they can also be configured to be sent via the Event Forwarder as *task.error.logged* events.

Corrective Content

1. EDR Server 7.5.0 includes a security patch to Apache Solr to address CVE-2021-27905. [CB-35440]

2. Live Response

    a. A fix for a scenario in which text would not immediately wrap in the Live Response command line interface upon being typed or pasted in; It would only wrap upon the user hitting enter. This has been improved in VMware Carbon Black EDR 7.5.0: Text is now immediately wrapped upon being typed or pasted into the command line interface so that the full content of the command is visible to the user before hitting enter. [CB-33290]

    b. A fix for a bug in which Live Response would error-out with a http-500 when the sensor client certificate starts with leading zeros, “00”. This has been resolved in VMware Carbon Black EDR 7.5.0: a user is now able to launch a Live Response session even if the sensor client certificate starts with “00”. [CB-34063]

    c. A fix for a bug in which a customer using Live Response via the API could create multiple simultaneous sessions for a single sensor. This has been resolved in VMware Carbon Black EDR 7.5.0: concurrent Live Response sessions on a sensor are prevented. [CB-27499]

    d. A fix for a bug in which a customer using Live Response, especially via the API, could queue a new command in a session that was very recently closed by a previous request, causing the subsequent command to sit in a “Pending” state, rather than update to “Cancel”. This has been resolved in VMware Carbon Black EDR 7.5.0: we have implemented a stricter mechanism to prevent commands

from being submitted to a closed Live Response session, with an error message of, “Command cannot be run as session is being closed.” [CB-27507]

e. A fix for a bug in which, if a customer submits a POST request to /api/v1/cblr/session with the sensor_id in the form of a string instead of an integer, Live Response will appear to create a session for the specified sensor, but the session will stay in a pending state indefinitely. Additionally, the pending session cannot be closed via the API nor the UI. This has been resolved in VMware Carbon Black EDR 7.5.0: if there is no session_id in the API POST payload, a 400 error code will be returned with an error message of, “sensor_id not provided”, and if there is a string instead of an integer in the API POST payload, a 400 error code will be returned with an error message of, “Invalid sensor_id provided, integer expected”. [CB-24759]

f. A fix for a scenario in which typing “help files” in the Live Response command line interface would return the following: “files [-s session id] [action] [options], which is not helpful nor usable for the customer since the available actions and options are unclear. This has been improved in VMware Carbon Black EDR 7.5.0: entering ‘help files’ now returns the available actions and information about the session ID and the options, global vs. session scope. [CB-4604]

g. A fix for a bug in which file content can fail to render if the content of the target file consists of a single line of text in between two double quotes, i.e. “carbonblack”. This has been resolved in VMware Carbon Black EDR 7.5.0: file contents are properly fetched via Live Response for all files, including those that contain a single line of text in between double quotes. [CB-32472]

h. A fix for a bug in which a Hexdump of a file can fail to render if the content of the target file consists of a single line of text in between two double quotes, i.e. “carbonblack”. This has been resolved in VMware Carbon Black EDR 7.5.0: Hexdumps are properly fetched via Live Response for all files, including those that contain a single line of text in between double quotes. [CB-35021]

3. Site Throttling

a. A fix for a bug in which a day-of-the-week value outside of the valid 0-6 range would be accepted for Site Throttling, if specified via the API. This has been resolved in VMware Carbon Black EDR 7.5.0: Day-of-the-week values <0 and >6 are no longer accepted and the system now responds with a 400 error and an appropriate error message when presented with an out-of-range day-of-the-week value for throttling. [CB-19571]

b. A fix for a bug in which an hour-of-the-day start time value outside of the valid range would be accepted for Site Throttling, if specified via the API. This has been resolved in VMware Carbon Black EDR 7.5.0: the system now responds with a 400 error and an appropriate error message when presented with an out-of-range start time value for throttling. [CB-19572]

c. A fix for a bug in which a bytes/second value outside of the valid 1-2,097,151 KB/second range would be accepted for Site Throttling, if specified via the API. This has been resolved in VMware Carbon Black EDR 7.5.0: KB/second values <1 and >2,097,151 are no longer accepted and the system now responds with a 400 error and an appropriate error message when presented with an out-of-range bytes-per-second value for throttling. [CB-19568]

d. A fix for a bug in which an overly large bytes/second value for Site Throttling would improperly generate a 500 error response in the UI. The UI only allows bytes/sec between 1 and 2,097,151 KB. If you specified a larger value (i.e. 2,097,200 KB) in the UI, the backend would respond with a 500 error. This has been resolved in VMware Carbon Black EDR 7.5.0: the system now responds with a 400 (BAD REQUEST) error along with an appropriate error message when presented with a bytes/second value that is too large. [CB-19570, relates to CB-19568 above]

e. A fix for a bug in which an hour-of-the-day start time value that is equal to or greater than the hour-of-the-day end time value would be accepted for Site Throttling, if specified via the API. The result of this scenario was a call that "succeeds" with an empty return ID. If this blank return ID is then used for a 'get' call, the system would respond with a 404 error. This has been resolved in VMware Carbon Black EDR 7.5.0: the system now responds with a 400 (BAD REQUEST) error along with an appropriate error message when presented with an out-of-range end time (that is equal to or less than the start time) for throttling. [CB-19574]

4. Change of "OSX" to "macOS" in the UI - Occurrences of "OSX" in the UI have been updated to "macOS" to align with Apple's updated nomenclature. Please note that process and binary search queries will still contain "osx", as this is how the data is stored. [CB-34891]

5. Prior to this fix, a feed creation attempt would fail with a 500 response if the JSON code for the feed at the specified URL included a non-string category. VMware Carbon Black Server 7.5.0 corrects this behavior by returning a 400 response with an appropriate error message in this scenario. [CB-33360]

6. Prior to this fix, the Process Analysis page did not resolve SHA256-based hits on the Alliance Feed Report section of the UI. When we introduced support for SHA-256 process hashes, we neglected to update the Alliance Feeds section of the metadata panel on the Process Analysis page to display hits for feeds that include SHA-256 IOC values. This has been resolved in VMware Carbon Black EDR 7.5.0. [CB-31341]

7. Prior to this fix, customers could receive alerts and see exclamation symbols in the Process Analysis page for an Indicator of Compromise (IOC) that they elected to ignore and/or for a Threat Report that they elected to disable. This has been resolved in VMware Carbon Black EDR 7.5.0: Alerts will not be sent and exclamation symbols will not be shown for events associated with ignored IOCs and disabled Threat Reports. [CB-27722]

8. A fix for a scenario in which certain new events would automatically populate as tagged in the UI, when they should not. This has been resolved in VMware Carbon Black EDR 7.5.0: new events will no longer be tagged automatically in the UI. [CB-33630, CB-33666]

9. A fix for an inconsistency in the product in which negative Threat Report scores (scores range from -100 to 100) would be displayed as positive, absolute values on the Process Analysis page. This has been resolved in VMware Carbon Black EDR 7.5.0: negative Threat Report scores are now properly displayed as negative values on the Process Analysis page. [CB-32983]

10. A fix for a bug in which a cbcluster task (start/stop/status) can hang due to multiprocessing. This has been resolved in VMware Carbon Black EDR 7.5.0: cbcluster tasks should no longer hang. [CB-33788]

11. A fix for a bug in which the command, “cbcheck scan-logs”, does not find all of the <err> events in the coreservices/debug.log. This has been resolved in VMware Carbon Black EDR 7.5.0: execution of “cbcheck scan-logs” finds all errors that have not been excluded. [CB-33716]

12. Upon stopping the cb-rabbitmq service, the Erlang Port Mapper Daemon (EPMD) process is now also stopped, to improve system stability. [CB-33312]

13. Some EDR Java-based services (cb-datastore, cb-solr, and cb-datagrid) are subject to a bug in the third-party logback library, such that temporary files with the extension ".tmp" are sometimes left in their respective log directories. In EDR Server 7.1, we added a cron job to clean up these files periodically for cb-datastore, but this job does not work if the log directory is a symlink to a different directory location. This has been resolved in VMware Carbon Black EDR 7.5.0: with this fix, we have improved that cron job and

added two new additional jobs, so that all three services are covered. Stray .tmp files will be cleaned up daily, even if the log path is a symlink. [CB-22730]

14. A fix for a bug in which Solr ingestion could halt. This has been resolved in VMware Carbon Black EDR 7.5.0: we patched Solr 8.6.3 with a fix provided in Solr 8.8.2, which prevents Solr ingestion from stopping completely. [CB-35332]

15. A fix for a bug in which an attempt to add a new cluster node using a non-default user would fail with an error indicating missing sudo permissions. This has been resolved in VMware Carbon Black EDR 7.5.0: a non-root user can now successfully add a new cluster node. [CB-18417]

16. A fix for a bug in which the movement of sensors to a new group would trigger Duo two-factor authentication. This has been resolved in VMware Carbon Black EDR 7.5.0: The only operations which will trigger two-factor authentication are now Login, initiating a Live Response session, and adding or removing Network Isolation from a sensor. Other operations that update sensor settings via the /api/v*/sensor endpoint, such as moving sensors between groups, will no longer trigger two-factor authentication.

    Please note that, while modifications to the Duo plugin file at /usr/share/cb/plugins/duo/duo_2fa_auth_callback.py are not officially supported, if any customer has modified that file or relocated it by changing the value of the TwoFactorAuthCallbackModulePath cb.conf setting, then the upgrade could cause problems with logging in and performing other actions. We do not expect customers to run into this problem since we believe all or most customers have not made changes to this file. However, we wanted to call it out in a release note since it is theoretically possible. Also, please note that this does not affect Hosted EDR instances. If a customer *does* happen to run into this issue, it would be resolved by setting the TwoFactorAuthCallbackModulePath setting back to the default value of /usr/share/cb/plugins/duo/duo_2fa_auth_callback.py. Any customizations applied to this file originally would need to be re-applied. [CB-34129]

17. A fix for a bug in which, if a request to the /internal/api/sensor/queued/<int:sensor_id> endpoint is made very soon after the referenced sensor has checked in, either no data will be retrieved, or the data retrieved may be stale. This has been resolved in VMware Carbon Black EDR 7.5.0: SensorQueuedDataStats data is now available as soon as it is retrieved upon sensor check-in. [CB-32648]

18. A fix for a bug in which, if a user attempts to export a CSV file (‘Export’ dropdown > ‘Export all’, ‘Export visible’) of sensors when no sensors are selected, an error of “sensor.html Failed - No file” is returned in the Downloads bar of the browser. This has been resolved in VMware Carbon Black EDR 7.5.0: now, the CSV file will still download,

but it will only display the column headers, without any rows of results, if no sensors were selected. [CB-29801]

19. A fix for a broken link on the Sharing Settings page: the link to https://www.vmware.com/help/privacy.html used to be broken and take users to a 404 Error - Page not found at a different address, https://www.carbonblack.com/solutions/carbon-black/collaboration/. This has been resolved in VMware Carbon Black EDR 7.5.0: the link now takes users to the correct address, https://www.vmware.com/help/privacy.html. [CB-33451]

20. Enhancements to CbDiags with collection of additional data to enable improved troubleshooting. [CB-32241, CB-34075]

Third Party Software Updates

1. Jetty: 9.3.41 → 9.4.39
2. PostgreSQL: 10.15 → 10.16
3. Python: 3.8.7 → 3.9.5
4. Redis: 6.0.6 → 6.0.9 (EL6), 6.0.13 (EL7 & EL8)
5. Underscore.js 1.8.3 → 1.12.1

Known Issues

1. When a Server 7.5.0 license is applied for the first time or reapplied, sensor check-ins may fail with an “invalid license” error for approximately the first 20 seconds, then succeed. [CB-35684]

2. In Server 7.5.0, on the Search Threat Reports page, searching for a range of IP addresses (Add Criteria > IP address > enter a range of network addresses) is broken. The query attempt will repeat indefinitely but never successfully complete until the user forces it to stop or closes the browser. [CB-35676]

3. In Server 7.5.0, the export of Process Analysis events does not work properly for an export of a large number of events (> ~50). If a user clicks on the ‘Actions’ drop-down and clicks ‘Export events’, with ~50 or more events selected, the CSV export will contain no data or very limited, incomplete data. This is a new issue introduced in Server 7.5.0. [CB-35675]

4. In Server 7.5.0, on the Triage Alerts Page, an invalid search with malformed syntax fails silently, without an error message. In previous versions, an invalid query would return an error message of “Malformed syntax in search query.” Via the API, a malformed query submitted on Server 7.5.0 returns a 500 error with no error message, whereas a malformed query submitted on previous versions returns a 400 error with the “Malformed syntax in search query.” error message. [CB-35669]

5. In Server 7.5.0, in the Configure Watchlist Expiration panel on the Watchlists page, a whole number must be entered for the watchlist expiration duration in order to save, even when the first option, “Do not mark watchlists as expired if they have no hits.” is selected. The configuration should successfully save when “Do not mark watchlists as expired if they have no hits.” is selected and the “Notify me when watchlists have not received hits in” value is blank. [CB-35668]

6. In Server 7.5.0, a user with “No Access” to a particular sensor group will experience an infinite loading indicator on the Live Query page when they try to execute a Live Query that includes that sensor group. [CB-35335]

7. In Server 7.5.0, when clicking on a link in the header of the Process Analysis page to go to the corresponding Process Search result, the Process Search does not execute automatically upon entering the Process Search page. The user has to click the “Search” button for the Process Search to execute, which is a new behavior. [CB-35313]

8. In Server 7.5.0, the naming conventions for sensor groups are now limited to Alphanumerics, spaces, and underscores, but the UI indicates that hyphens are still allowed, which they are not. [CB-35153]

9. In Server 7.5.0, when using the `GET/v1/process/{guid}/{segmentid}/preview` API, process information is not properly returned. [CB-35148]

10. In Server 7.5.0, when using the `GET /v3/{guid}/event` API (or `GET /v5/{guid}/event`), submitted child process events of type "2" (other exec) do not properly store the process PID. [CB-35147]

11. In Server 7.5.0, Binary Search searches can sometimes return zero results when there are matching results that should be returned. [CB-35139]

12. Beginning in Server 7.4.0, creation of a Watchlist from the Binary Search page parses the search terms incorrectly: the search terms are combined with ANDs instead of ORs, and ignores parentheses. [CB-34976]

13. Beginning in Server 7.4.0, in the Process Analysis events list, “Crossproc” events that are marked with the tamper flag should also display a red dot, like other tamper events,

but they do not. Also, in Process Search, there should be a red dot in the process' Hits column for a process that has a tamper flag, but there is not. [CB-34964]

14. In Server 7.5.0, on the Process Search page, a process that has a Threat Intelligence Feed hit tag in one segment may not display the feed hit icon (a red dot) when "Group by process" is selected. [CB-33586]

15. In some cases, a process Watchlist will produce more hits than alerts. When a Watchlist query is executed using the original terms (e.g. process_name:notepad.exe), both the original segment (with events) and the tagged segment (without events) are returned, and both results appear on the Watchlists page. This makes it appear that there have been two hits, when in fact, there was only one. The result is two apparent hits, but only one alert, which is deceptive. [CB-33355]

16. cb-enterprise fails to install on RHEL/CentOS 8 with FIPS 140-2 enabled, which is due to a change in Red Hat 8 that affected Paramiko (https://bugzilla.redhat.com/show_bug.cgi?id=1778939). The workaround is to use RHEL/CentOS 7 if you enable FIPS 140-2. [CB-33352]

17. Live Query fails to take the `SensorInactiveFilterDays` setting into account when determining which sensors to target. The sensor count on the right side of the 'Current query' bar shows all targeted sensors, while the quantity of targeted sensors in the 'Run New Query' pop-up does account for `SensorInactiveFilterDays`, and will sometimes show a lower number. [CB-31136]

18. For Server versions 6.x.x - 7.2.0 (all versions which include Apache Solr 6.x), a bug in Apache Solr 6 (https://issues.apache.org/jira/browse/SOLR-9882.) causes incomplete results when `partialResults=True`. The Pagination bar, together with a large number, will appear on the Process Search page as a result of a search. However, only a few or even zero actual documents are displayed. [CB-30074]

    The fix for this issue has not yet been validated in Server 7.3.0 +, based on Apache Solr 8.

19. Any modification, creation or deletion of files inside C:\Windows\CarbonBlack will create Tamper Alerts with empty "Tamper Type" fields on the Triage Alerts page due to file modifications inside the Windows sensor's working directory. [CB-27698]

20. The Process Analysis page displays a destination IP of "0.0.0.0" for a network connection event if the sensor is interacting with a proxy server, when instead, it should display no IP address. [CB-25085]

21. 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 that contains SHA-256. When a user clicks the link, the binary store shows no SHA-256. [CB-24519]

22. 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, and re-enable the custom email server. [CB-20565]

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

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

25. For Server versions 6.x.x - 7.1.0, which include Apache Solr 6.x, Process Searches using `*_md5,md5, *_SHA256, SHA256` are case-sensitive. These searches were case-insensitive in pre-6-series Server versions, which include Apache Solr 5.x. [CB-14311]

    This issue is resolved in Server 7.1.1 +.

26. When creating a watchlist from a Threat Feed, VMware Carbon Black EDR incorrectly creates the query and the watchlist does not run – it creates an error. To see if your watchlist formed an error, check the status on the Watchlist page. As a workaround, the VMware Carbon Black EDR 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.

Contacting Support

VMware Carbon Black EDR 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 (VMware Carbon Black EDR server and sensor versions)
- **Hardware configuration:** Hardware configuration of the VMware Carbon Black EDR 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 you review the related content on the User Exchange and the new release documentation location, the Carbon Black EDR section of docs.vmware.com.