Carbon Black.

Cb Response Windows Sensor

Release Notes

Version 6.1.2

November 2017

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

Web: http://www.carbonblack.com

Introduction

The *Cb Response Windows Sensor v6.1.2 Release Notes* document provides information for users upgrading from previous versions as well as users new to the product. It consists of the following major sections:

Corrective Content – Describes issues 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.

Technical Support – Describes ways to contact Carbon Black Technical Support and details what information to have ready.

This document is a supplement to the main Cb Response product documentation.

Purpose of this Release

The Cb Response Windows Sensor 6.1.2 release contains *support for IPv6 netconn events, support for Windows ODX, performance improvements, and additional bug fixes*.

Note: Cb Response sensor releases are cumulative and include all changes and fixes from previous releases.

Documentation

The standard product documentation for Cb Response includes:

- *Cb Response User Guide* – Describes Cb Response feature functionality in detail, plus administrative functions.
- *Cb Response Server Sizing Guide* – Provides details on infrastructure sizing for Cb Response server.
- *Cb Response API* – Documentation for the Cb Response API is located at https://developer.carbonblack.com.

Additional documentation for specialized tasks and situations is available on the Carbon Black User eXchange at https://community.carbonblack.com/.

Sensor Operating Systems

For the most up-to-date list of supported operating systems for Cb Response sensors (and all Carbon Black products), refer to the following location in the Carbon Black User eXchange:

https://community.carbonblack.com/docs/DOC-7991

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 upgrade process. Our Professional Services organization is also available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

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

Corrective Content

This Cb Response Windows Sensor release (6.1.2.71109) provides the following corrective content changes:

1. [NEW] Added support for capturing IPv6 netconn events. (CB-9386, CB-9507)
2. [NEW] Windows sensor now supports Windows ODX. (CB-13045, CB-13474, CB-14380)
3. Updated OpenSSL to version 1.0.2m, and updated LibCurl to version 7.56.1. (CB-16455, CB-16329)
4. Fixed bug with uninstalling a GPO install of sensor from Add/Remove Programs menu. (CB-12702)
5. Fixed bug with read/write lock creating deadlock condition. (CB-13021, CB-13139)
6. Fixed an issue with NULL pointer dereferences on inaccessible file paths. (CB-13192, CB-13482, CB-14704)
7. Fixed bug with retrieving system paths causing deadlock issues. (CB-13259, CB-13485)
8. Fixed an issue with StreamContext where driver verifier was returning NULL for small memory allocations. (CB-13813)
9. Fixed an issue relating to TLS validation between sensor and server. (CB-14028)
10. Improved security with driver communications. (CB-11596)
11. Fixed bug resulting in memory leak issues. (CB-13010, CB-13484)
12. Fixed an issue where GPO upgrades resulted in multiple sensor IDs. (CB-13136)
13. Fixed a bug where retrieving the system path in certain conditions created a possible deadlock. (CB-13259)
14. Improved sensor installer to check for Base Filtering Engine service at install. (CB-13334)

15. Fixed an issue where Cb directories were not being removed after uninstalling the sensor. (CB-9604)
16. Fixed an issue with calculating total disk space used for file store. (CB-12260)
17. Fixed issue with setting registry key for StoreDiskQuotaMb. (CB-12434)
18. Fixed an issue with incorrect dialog box appearing when uninstalling sensor. (CB-13164)
19. Fixed an issue with **uninstall.exe** not removing Cb from Add/Remove Programs. (CB-13252)
20. Fixed an issue with multiple Cb entries appearing in Add/Remove Programs. (CB-13313, CB-13373)
21. Fixed an issue with upgrading sensor using a different install method than current version. (CB-13375, CB-13438)
22. Fixed an issue with disabling CBLR commands in sensor.log file. (CB-13767)
23. Fixed an issue with excessive handle counts being reported. (CB-13972)
24. Fixed an issue with the Cb icon displayed in Process Analyze page. (CB-13256)
25. Improved file system queries on network drives. (CB-14210)
26. Fixed bug with taking Windows system backups by updating the service image path of the .exe install to use system root path. (CB-14360)
27. Fixed a bug with Stream Context in which driver verifier was returning a NULL value for small memory allocations. (CB-14360)
28. Fixed a bug in which cross proc callback routine was creating a deadlock condition. (CB-14626)
29. Fixed a bug in which Unicode characters in the host name prevented registering the sensor. (CB-14809)
30. Fixed a bug in which the Windows sensor was not honoring the Retry-After header that is returned when the /data/eventlog/reserve API call returns a 503 error. (CB-15259)
31. Fixed a bug where NULL filenames were creating invalid memory references and creating BSOD. (CB-15437)
32. Fixed a bug in which cbk7.sys pre-write filter attempts to read a write buffer without validation creating potential BSOD. (CB-15635)

Known Issues and Limitations

Cb Entries Remaining in Add/Remove Programs

Customers uninstalling their Cb Response Windows sensor through **uninst.exe** will notice remaining Cb entries in the Add/Remove Programs window.

Cb Branding Is Different Between MSI and EXE Installers

Customers using the Add/Remove Program window to manage their Cb Response installation should be aware that the Cb branding between the MSI and EXE installers is different.

Disproportionate Cb Logo on Install Wizard

Customers running the .exe installer may notice a disproportionate Carbon Black logo appearing on the install wizard.

Install/Uninstall & Upgrade/Downgrade of Sensor on WinXP Requires Reboot

Customers running the Windows sensor on a Windows XP machine should note that a reboot of the machine will be required for all install/uninstall and upgrade/downgrade methods in order to successfully load and unload Cb drivers.

Cb Protection Upgrade Needed

Customers running Cb Protection to tamper-protect the Cb Response Sensor, and who do not opt-in to CDC will need to update their tamper rule settings for Cb Protection to the latest “Cb Response Tamper Protection” Rapid Config (if running CbP 8.0) or Updater (if running CbP 7.x) in order to successfully upgrade/downgrade their Cb Response sensor. Please contact technical support to obtain the latest Rapid Config or Updater for Cb Protection.

Contacting Technical Support

Carbon Black Technical Support provides the following channels for resolving support questions:

Technical Support Contact Options
Web: www.carbonblack.com
Email: support@carbonblack.com
Phone: 877.248.9098 (877.BIT9.098)
Fax: 617.393.7499
Hours: 8:00 a.m. to 8:00 p.m. EST

Reporting Problems

When contacting Carbon Black Technical Support, be sure to provide the following information:

Required Information	**Description**
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 of the manual you are using. The date and version of the document appear after the copyright section of each manual.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement