Carbon Black Cloud

Release Notes

Windows 3.4.0

These release notes apply to Carbon Black Cloud Windows sensor version 3.4.0.1097. Only issues that have been fixed since the maintenance release version 3.4.0.1086 are included in these release notes. Known issues are maintained in this document, but are the same as the earlier version.

Notes:

- The 3.4 MSI is signed with a SHA256 signature. Support for SHA256 was provided as part of a Windows 7 patch. If Windows 7 machines or Windows Server 2008 R2 machines do not have this patch, it can be found here: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/3033929. Machines running later operating systems have out-of-the-box support.

- Windows 7 requires SHA256 signing as of July 2019. See https://support.microsoft.com/en-us/help/4474419/sha-2-code-signing-support-update.

- Customers who are upgrading to Windows sensor version 3.4.0.1093 from previous 3.4 sensor versions must ensure that the policy setting **Deny/Terminate Unknown application or process that Runs or is running Deny** is disabled or not in place. Please see the Knowledge base article: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-Sensor-Upgrade-from-3-4-x-x-fails/ta-p/73366. This issue was observed internally, and only fails intermittently. However, Carbon Black recommends that you disable this policy setting to ensure successful upgrades.

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	Description
UAV-1290	A crash was reported internally on one OS: Windows 10 RS 5 x64 in 3.5.0.1373.
DSEN-6757	One customer reported that the 3.4.0.1086 sensor intermittently crashed Outlook or caused delays.

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

DSEN-6876, DSEN-4232	In Windows sensor version 3.4.0.1086, some Microsoft applications had slow performance.
DSEN-6322, EA-14880	Short delays were occurring when opening various Office files and navigating through file systems on Windows 10.

Known issues

Issue ID	Description
DSEN-1987	False positive alert when the [application name] attempts to access the raw disk on the file. See https://community.carbonblack.com/docs/DOC-10730.
DSEN-1180, DSEN-3065	When using Live Response, users can terminate the sensor if they terminate `RepMgr.exe`. Terminating this process means that the sensor cannot connect to the backend and the Live Response session ends. The sensor does not recover until after a reboot. Users can delete certain files within the confer directory. Users are advised to use caution during Live Response sessions.
DSEN-2378	During direct invited install, Windows installer shows a blank error dialogue when attempting to install on an unsupported OS.
DSEN-1387	Background Scan remains disabled on devices where VDI=1 was used. See https://community.carbonblack.com/docs/DOC-12001.
DSEN-3061	Sensor does not whitelist files by certificate if it is signed with multi-byte characters.
DSEN-4216	The 3.4 sensor accumulates deleted files within the sensor cache and does not remove them when the files are removed from disk. This can lead to the sensor reporting that malware is still on disk when it has been removed.
DSEN-4050	If a user executes an unattended install with the flag and argument "`INSTALLFOLDER=<path>`", the sensor will install and be non-functional. Carbon Black does not support non-default install paths.
DSEN-4043	Under high load, the sensor might experience an issue where `repmgr.exe's` handle counts grow very large; this can cause minor performance issues.

DSEN-4143	Users might experience blocks of Microsoft OS upgrades. An admin can workaround this issue by either placing the sensor in bypass or adding the following paths to bypass: 1. `**\windows\servicing\**` 2. `**\$windows.~b\**` Make sure that the policy configuration **When an unknown application tries to run - deny/terminate** is disabled when you upgrade.
DSEN-3992	Subkeys can be created under the CBDefense key in the Windows registry.
DSEN-4054, DSEN-4033	The LiveResponse memdump command can cause crashes. It is disabled by default on Windows sensors 3.3 and above. Instructions on enabling the command can be provided by your support representative.
DSEN-4375	The sensor can write 290MB of data to `confer.log` over the course of nine hours. `Confer.log` is expected to be much smaller.
DSEN-4591, EA-13682	Arcmap files are corrupted or missing in certain environments.
DSEN-4581, DSEN-4694	A terminate action might be applied to `wmiprvse.exe`, and a corresponding alert might display in the Carbon Black Cloud console during machine start-up. At the time, `wmiprvse` has an unknown reputation and is scraping `lsass.exe`. This commonly happens during Windows updates. `Wmiprvse.exe` should execute after the reputation resolves; the update should succeed.
DSEN-4756, DSER-14090, EA-13906	Customers who are running CB ThreatHunter as a standalone implementation might see the Windows Security Center Real Time protection feature disabled. You can resolve this issue by going to the **Policies** page, clicking the **Sensor** tab, and unchecking **Use Windows Security Center** (then click **Save**).
DSEN-5493, DSEN-5491	During updates to Windows 1H19, the system either blocks the update or potentially crashes during the update. This issue was found internally, and the issue does not reproduce if the sensor is in bypass mode.
DSEN-4924 EA-13414	Interoperability issues can occur with Skype on Windows 7. Other operating systems are unaffected.
EA-14455, DSEN-5699	The install of the sensor has been observed to fail on Windows Server 2019 when there is a missing directory value for registry key `HKLM\SYSTEM\CurrentControlSet\Control\EarlyLaunch value "BackupPath"`. The value is typically `C:\Windows\ELAMBKUP`.

DSEN-5626	The sensor does not prevent copy operations on Known Malware or Blacklisted files that have been quarantined.
DSEN-5934, EA-14272, EA-14596	Opening attachments while using applications such as KnowBe4 Second Chance or Digital Guardian's Outlook plug-in can fail.
DSEN-6372	If the sensor's background scan goes directly from **disabled** (either via install arguments or policy) to **expedited**, a race condition can put the background scan into a disabled state. This issue has only been identified internally, and has not been observed externally.
DSEN-5163	The sensor does not prohibit downgrades from existing 3.4 versions to older 3.4 versions. The team does not recommend a downgrade between 3.4 builds.
DSEN-3408	The "`CLI_USERS=<Sid>`" command line option works correctly when you install non-interactively using a `COMPANY_CODE`, but it doesn't work if you use the direct user installation method.