PSC sensor version 3.4.0.1070 is for Windows only. Please note that only issues fixed since the maintenance release version 3.4.0.1061 are included in these release notes. Known issues are maintained, but should be 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 there are Windows 7 machines or Windows Server 2008 R2 machines that 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 will require 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 the 3.4.0.1070 from previous 3.4 sensor versions must ensure that the policy setting **Deny/Terminate Unknown application or process that Runs or is running Deny** should be 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. Note that 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
DSEN-5801, EA-14475	There has been one observed case of registry heavy applications causing CPU overhead. This issue is now resolved.
UAV-1160, EA-14700	A small percentage of watchlist hits have been reported as false positives. One customer has reported this issue thus far. This issue is now resolved.

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

DSEN-6276	This issue was found internally. The fix improves the SCCM deployment experience for customers running CB Threat Hunter only. CB Defense customers are unaffected.

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 PSC sensor if they terminate `RepMgr.exe`. Terminating this process means that the sensor cannot connect to the back end and the Live Response session ends. The sensor does not recover until after a reboot. Users can also delete certain files within the confer directory. Users are advised to use caution during Live Response sessions.
DSEN-2378	During an attended 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. This issue will be resolved in the 3.5 release.
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. This issue will be resolved in 3.5.
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. This issue will be fixed in the 3.5 sensor.
DSEN-4375	The sensor has been observed to write 290MB of data to `confer.log` over the course of nine hours. `Confer.log` is expected to be much smaller. This issue will be resolved in the 3.5 sensor release.
DSEN-4591, EA-13682	Arcmap files are corrupted or missing in certain environments.
DSEN-4581, DSEN-4694	You might see a terminate action applied to `wmiprvse.exe`, and an alert in the PSC 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 be able to execute after the reputation resolves, and the update should go through.
DSEN-4756, DSER-14090, EA-13906	Customers running CB ThreatHunter as a standalone implementation without CB Defense or CB LiveOps might see Windows Security Center Real Time protection feature disabled. This issue can be resolved by navigating to the **Policies** page, clicking the **Sensor** tab, and unchecking **Use Windows Security Center**.
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	Some customers have reported interoperability issues 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. in the case where 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 no longer prevents copy operations on Known Malware or Blacklisted files that have been quarantined. This fix is targeting the 3.5 sensor release.
DSEN-5995, EA-14707, EA-14723, EA-14729	Customers upgrading from 3.4.0.1016 to 3.4.0.1047 may see that Office applications such as Word and Excel will hang when updating a file on Google File Stream and similar products (Box, Citrix Cloud). This issue will be fixed in an upcoming 3.4 release.
DSEN-5934, EA-14272, EA-14956	Customers may have experienced the inability to open attachments while using applications such as KnowBe4 Second Chance or Digital Guardian's Outlook plug-in.
DSEN-6322, EA-14880	There have been intermittent reports of short delays when opening various Office files and navigating file systems on Windows 10.
DSEN-6372	If the sensor's background scan goes from **disabled** (either via install args or via cloud policy) directly to **expedited**, it's possible to hit a race condition which puts the background scan to disabled state. This 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 as it leaves the sensor in a bad state.