PSC sensor version 3.4.0.1047 is a Windows-only maintenance release that resolves issues seen in the field after the GA release of 3.4.0.1016. This document only lists issues that have been fixed since the GA release.

For the full set of features and issues fixed in for the GA release of minor version 3.4, please see:
https://community.carbonblack.com/t5/CB-Predictive-Security-Cloud/Announcing-the-3-4-Windows-PSC-Sensor-General-Availability/m-p/72982#M124

Notes:

- The 3.4 sensor files are signed with a SHA256 signature. Windows 7 and Server 2008 R2 machines will not accept the SHA256 digital signatures without the following patch : 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 upgrade to the sensor versions 3.4.0.1016 or later 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. 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-5500	Previously, a policy rule was needed on 19H1 machines to avoid blackscreens and hang ups on user login and logout. This policy rule is no longer needed, and should be removed after all your 19H1 agents are running 3.4.0.1047 or higher. See https://community.carbonblack.com/t5/CB-Predictive-Security-Cloud/Update-Compatibility-with-the-Upcoming-Windows-OS-Update-1H19/m-p/72983#M125.
DSEN-5511, EA-14242	One customer observed an issue where endpoints caused .net applications to deadlock. This issue is now fixed.
DSEN-5677	Previously, the sensor required an uninstall and fresh install to apply the `CURL_CRL_CHECK` flag. The sensor upgrade can now accept that flag when upgraded via the command line. This `CURL_CRL_CHECK` flag was fixed in 3.4.0.1016 via DSEN-5002. See this KB on disabling CRL checking for more information: https://community.carbonblack.com/t5/Knowledge-Base/CB-Defense-How-To-Configure-Sensor-Not-To-Require-CRL-Checks/ta-p/73036
DSEN-5480	Previously, the team internally observed an issue that results in a failure of the API Bypass feature under the following two joint conditions: 1. Prevention policy to deny running from the path `c:\test\*` 2. A Bypass rule is applied when `c:\test\calc.exe` performs any operation. You could work around this issue by applying Bypass to `c:\test\calc.exe` when it “runs or is running”. This issue is now fixed.
DSEN-5377	Previously, running an attended upgrade while the sensor is in Bypass mode using a non-Admin CMD prompt resulted in an incomplete uninstall during the upgrade process. This could leave the system in a state in which the sensor could not be re-installed. This issue is now fixed.
DSEN-5371	Previously, moving in and out of bypass via RepCLI or the tray icon could cause resources to hang on the endpoint. This issue is fixed.

Carbon Black.

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, you can terminate the PSC sensor if you 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. You can also delete certain files within the `confer` directory. You 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 a future 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 removed malware is still on disk.
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` handle counts grow very large; this can cause minor performance issues.
DSEN-4143, DSEN-5493, DSEN-5491	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.

	Less frequently, crashes can occur on the endpoint during an OS upgrade. You can place the sensor into full bypass if issues are still experienced.
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 sensor 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 excessive log data. This issue will be resolved in the 3.5 sensor release.
DSEN-4591, EA-13682	Arcmap files are corrupted or missing in certain environments. This issue has been observed very infrequently.
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-4924 EA-13414	Some customers have reported interoperability issues with Skype on Windows 7. Other operating systems are unaffected.
EA-14455, DSEN-5699	Sensor install has been observed to fail on Windows Server 2019. The issue can happen on Windows 10 as well, though that has not been observed. The issue manifests 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-5105, EA-14012	There have been a few observations of CPU spikes on customer endpoint. These CPU spikes occur when the certificate whitelist is updated. The issue has been infrequent. This fix is targeting the 3.5 sensor release.
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).
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-5801, EA-14475	There has been one observed case of CPU increase related to running explorer.exe on a virtual server.