Cb Defense

Cb Predictive Security Cloud

Release Notes

September 2018

General Notes

Cb Defense Sensor version 3.2.1 is a GA (General Availability) release for macOS only.

Important

If a sensor is not upgraded to the latest 3.2.1 version **before** upgrading to 10.14 Mojave, the sensor enters bypass mode on 10.14 until sensor upgrade.

Devices upgrading from versions **3.0** and older to **3.1** and newer (including **3.2.1**) should have new code signing certificate (***Team ID 7AGZNQ2S2T***) whitelisted prior to sensor upgrade. The procedure is required due to a Team ID change in the Cb Defense code signing certificate introduced in 3.1 release. Please see Caveats section for more details. Carbon Black recommends using an MDM-compatible mass deploy solution to push the updates, pre-approve, and whitelist the KEXT code signing certificate.

Release Checksums

3.2.1.10 DMG SHA256 Checksum	36b5c422196a2f1e35385121b0c7dfc5311dea1125ce765bf8482280f3bb8b05
3.2.1.10 PKG SHA256 Checksum	17af7d17342955fe5ee1d28eab3b63f26248cf7893b716d127b647aae787fb1a

New Features

10.14 Mojave Support

This sensor version supports the latest version of macOS, 10.14 Mojave.

PKG Installer Whitelisting

This new feature extends certificate whitelisting functionality to support Mac PKG installers alongside the previous capability to whitelist binary certificates. You can whitelist PKG installer files by a verified installer certificate, and any code files that are part of the installer package (such as pre/post install scripts or installed executable code) inherit initial trust (get LOCAL_WHITE reputation assigned), even if the files themselves are not signed or NOT_LISTED. Such whitelisting capability lets you whitelist common installers that are pushed by software deployment tools. This lets you achieve successful install/upgrade deployments, even with strict prevention rules in place. For more information about how to use this feature, please see the following Knowledge Base Article.

Mass Sensor Management

Mass sensor management enables policy assignment for groups of sensors based on Organizational Unit, subnet, domain name, and device name. The feature enables auto-assignment of new sensors into existing sensor groups and policy updates for groups of sensors. For more information about this feature, see the Cb Defense User Guide.

Issues Resolved in sensor version 3.2.1 (since 3.1.1)

Efficacy Enhancements and Bug Fixes

ID	Description
DSEN-3053	Extended behavioral ***REVERSE_SHELL TTP*** detection also detects ***Empyre*** reverse shells and similar kinds.
DSEN-2468	Enhanced Ransomware detection heuristics increase detection accuracy of not-in-place file encryption.
DSEN-3569	***PORTSCAN TTP*** is now flagged detecting a connection attempt from a port scanning host. The event is associated with the *repmgr* process that detects the port scan.
DSEN-2523	DMG image files code signing signatures are now detected and reported on the **Application** tab.
DSEN-2677	Improved dyld code injection detection and reduced false positives in cases

	where injection actor and target belong to the same application bundle (such as Firefox.app case).
DSEN-3012	Improved accuracy of certificate whitelisting for binary files during software upgrades. This fix especially applies to software upgrades where whitelisted code-signed files are copied and moved several times between staging locations. This can result in temporary file misclassification as unsigned. If the whitelisted application is distributed as a PKG installer, we recommend that you, in addition to whitelisting the binary, use the new ***PKG Installer Cert. Whitelisting*** feature and whitelist the trusted publisher of the PKG itself.
DSEN-3096	Resolved an efficacy issue when a policy did not sync correctly, which could lead to false positives or false negatives. The issue could occur under heavy loads, or for applications that started before a sensor install or upgrade.
DSEN-3011/ EA-12605 / TS-207	This fix resolves an efficacy issue, where prevention for malware persisted as a service and launched on OS boot several seconds late, thereby allowing malware or blacklisted application to initially run or make successful netconns.
DSEN-2999 / EA-12714 / TS-222 /TS-263	The fix resolves an efficacy issue identified with the *Entitle* malware, where malware that was delivered as a staged installer could be misclassified as pre-existing and terminated on post-execute instead of pre-execute.
DSEN-3097	The issue where the "Tries to run" -> "Terminate" rule was not terminating a pre-existing process is resolved.
DSEN-2968	Reduced false positives with “Invokes Untrusted” operation in a context of a script file that invokes another process.
DSEN-2964	Improved file-less script detection with perl one-liners.
DSEN-2963 / EA-12714	Improved detection of malware drop, handling cases where complex file IO operations can be leveraged to obfuscate the malware delivery. This improves prevention on pre-execute.

Performance and Stability

ID	Description
DSEN-2768	This issue mitigates sensor configuration file corruption after a hard OS shutdown that could lead devices to stop reporting to the cloud.
DSEN-3694	This issue resolves an interop issue between Cb Defense and the CCleaner utility, that could lead to kernel panic due to a tamper violation against Cb Defense service.
DSEN-2450	This issue resolves an issue in 3.1.1 where a rare Cb Defense sensor UI crash occurred when the sensor was uninstalled remotely by using the cloud console.
DSEN-2859	Optimized perceived user performance when the only prevention rules are string-based rules.

Other

ID	Description
DSEN-2214	Resolved a timing issue where a sensor that was configured with strict policy rules could block a sensor unattended upgrade. The issue did not apply to sensor upgrades that were initiated from the cloud console.
DSEN-1805	Resolved an issue where a policy update triggers an event and the reputation change is logged in the security log.
DSEN-2811	This issue cleans up Cb Defense-specific TimeMachine backup exclusions on sensor uninstall.
DSEN-3222	Resolved a vulnerability issue that was identified during pentesting that could lead to the disablement of Cb Defense bypassing uninstall protections using a specific code injection vector.
DSEN-2678	In addition to the PKG installer, Cb Defense installer DMG image is now code-signed by Carbon Black for compliance.
DSEN-2457	Added long command-line options to the customer-facing unattended uninstall tool.

Known Issues & Caveats

Description
The last (3.1) release introduced a new code signing certificate. The new 3.2 sensor requires KEXT approval to run upon a fresh sensor installation as well as an upgrade from 1.x or 3.0 sensor versions, but is not needed if upgrading from the 3.1 sensor version. If the devices are not provisioned with the approval, the sensor enters bypass mode. Carbon Black recommends using an MDM solution to push the approval. The following KB articles provide additional information. New KEXT bundle ID: com.carbonblack.defense.kext New Common name: Carbon Black, Inc. New Team ID: 7AGZNQ2S2T ➢ Cb Defense: How to approve Mac Sensor 3.0 KEXT for Install/Upgrade https://community.carbonblack.com/docs/DOC-12365 ➢ Cb Defense: Why does KEXT approval show Scargo Inc as Developer for new cert? https://community.carbonblack.com/docs/DOC-11891 ➢ Cb Defense: How to approve Mac Sensor 3.1 KEXT for Install/Upgrade https://community.carbonblack.com/docs/DOC-14333 ➢ Cb Defense: Why do I need to re-approve KEXT after upgrading to Mac Sensor 3.1? https://community.carbonblack.com/docs/DOC-14334 ➢ Cb Defense: Mac Sensor installs with status "Sensor Bypass Admin Action" https://community.carbonblack.com/docs/DOC-11997 ➢ Cb Defense: macOS 10.13.4 Kext Approval Changes https://community.carbonblack.com/docs/DOC-13277
Due to enhanced installer protections and a new reputation engine, downgrades from 3.2, 3.1 or 3.0 to 1.2 are not supported out-of-the-box. Contact Support if this downgrade is required. Uninstall and install is an alternative to a downgrade path; however, this process results in a new device ID and loss of linkage to the original device data. Please note that the downgrade from 3.2 to 3.1 or 3.0 are also subject to KEXT approval due to the certificate change.

Reminder: The **Live Response** feature on macOS does not currently include the memory dump command.

ID	Description
DSEN-2735	Device name in sensor management is case sensitive.
DSEN-2700	Rare issue where repmgr sporadically crashes on shutdown, typically when the network/cloud is unreachable.
EA-11120/2544	Certain environments can cause the sensor UI application to take focus of the local UI even when sensor UI is disabled. This is rare.
DSEN-2543	The unattended install script does not accept multiple long options. The workaround is to always provide a value (such as 0 or 1) next to every long option following = character, for example: `--downgrade=1 --skip-kext-approval-check=1`
DSEN-3740	When the device is removed from an AD domain, the sensor will still be reflected as within that domain in the **Endpoints** page and remain in a sensor group. The sensor must be taken out of auto-assignment to make policy updates to that sensor. As a workaround, you can manually remove the sensor from the AD group and assign a policy (click into the device, turn off auto-assign, and change the policy).
DSEN-3752	Cloud uninstall of the sensor takes a long time due to a change in the backend.