PSC sensor version 3.2.2.6 is a GA (General Availability) release for macOS only.

Important

Devices upgrading from versions **3.0** and older to **3.1** and newer (including **3.2.2**) 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 that was introduced in the 3.1 release. Please see the Known issues 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.

New features

This is a patch release to provide security enhancements and stability fixes. This sensor version supports the latest version of macOS, 10.14.1.

Release checksums

3.2.2.6 DMG SHA256 Checksum	018631ec37c6e0cc924f227c2f89cf3d9ef36afbfc176d056d31ce03f50bef57
3.2.2.6 PKG SHA256 Checksum	103490fe2000ad113b5f06f27afe1c388372dff4a07188e2b1c37d080403dc83

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	Description
DSEN-3859, DSEN-1334	This release fixes an issue where the rule "Invokes untrusted application" did not apply when the parent invoking the untrusted application was `/bin/sh`.
DSEN-3915	This release resolves an issue that was introduced in 3.0 that could cause sensor installation to fail after the device has been registered with the backend. The issue is limited to a small number of devices with a specific configuration.
DSEN-3914	This release includes safeguard improvements to prevent the accidental deletion of sensor files by admins when using the file delete feature.
DSEN-1170	This release fixes an issue where longer text entries were truncated in the sensor UI.
DSEN-3884	Minor vulnerability fixes.

Known issues

Description
The 3.1 release introduced a new code signing certificate. The 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 it is not needed if you are 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

Carbon Black.

➢ https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-How-to-approve-Mac-Sensor-3-0-KEXT-for-Install/ta-p/34012

➢ Cb Defense: Why does KEXT approval show Scargo Inc as Developer for new cert? https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-Why-does-KEXT-approval-show-Scargo-Inc-as-Developer/ta-p/38800

➢ Cb Defense: How to approve Mac Sensor 3.1 KEXT for Install/Upgrade https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-How-to-approve-Mac-Sensor-3-1-KEXT-for-Install/ta-p/49446

➢ Cb Defense: Why do I need to re-approve KEXT after upgrading to Mac Sensor 3.1? https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-Why-do-I-need-to-re-approve-KEXT-after-upgrading-to/ta-p/48057

➢ Cb Defense: Mac Sensor installs with status "Sensor Bypass Admin Action" https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-Mac-Sensor-installs-with-status-quot-Sensor-Bypass/ta-p/39730

➢ Cb Defense: macOS 10.13.4 Kext Approval Changes https://community.carbonblack.com/t5/Documentation-Downloads/macOS-10-13-4-Kext-Approval-Changes/ta-p/41490

Issue 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.
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 continues to be reflected as in that domain on the **Endpoints** page, and it remains 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.
DSEN-3752	Cloud uninstall of the sensor takes a long time due to a change in the backend.