Improvements

- Improved control panel SIGTERM recovery and restart logic.
- Improved ACS5000 panel firmware upgrade procedure to increase reliability.
- Made schedule activation more efficient reducing unnecessary device updates messages.
- Panel reboot now suppresses door forced and other hardware related events as a result of the paneld restart.

Fixes

- Fixed an issue where threat level processing was slowed down on accounts with a large number of schedules.

**BRIVO ONAIR 5.2.10 FIRMWARE
RELEASE NOTES
12/12/2018**

New Features

- ACS6000 and ACS300 control panels now support use of AD400 Wireless Locks and PIM400-485 units.
- Implemented functionality needed to pulse an Allegion AD400 Wireless Lock.
- Implemented support for AD400 Wireless Locks with keypads.
- Panels maintain the current state of their inputs and outputs through a controlled restart of the panel.
- Implemented new monitoring and reporting of magnetic tamper events for Allegion NDE Wireless Locks.

Improvements

- Added the ability to enable or disable network monitoring from the webCLI.
- Administrator username and passwords in webCLI no longer allow 'space', &, or # characters.
- Added detail memory usage for Brivo apps in the panel dump file.

Fixes

- Fixed an issue causing panel logs to show 'failed to sync hardware clock' messages.

Improvements

- Implemented CAN bus lockup detection logic as well as CAN bus recovery logic, allowing the control panel to detect an issue and then quickly resume normal operations after the recovery.
- Added the ability to enable or disable network monitoring from the webCLI.

Fixes

- Updated the CAN bus kernel and ensured it is backwards compatible with existing ACS6000 boards in the field.

Improvements

- Increased the maximum USB storage size to 8 GB
- Rebuilt the kernel with CAN bus driver in verbose mode
- Implemented the CAN bus recovery script which activates when noise is introduced on the CAN bus wiring.

Fixes

- Fixed an issue where momentary offline activity was being reported too frequently and this was changed to no longer report outages of less than 10 seconds. Additionally, only 2 consecutive missed heartbeat are reported.

Improvements

- Implemented an auto recovery mechanism to resolve communication between daughter and mother boards.
- During situations where a panel receives bad data, the monitoring software has been improved to prevent false alarms.
- Implemented processes to ensure that the new credential command operations (Update Credential and Delete Credential) do not run into panel/server communication conflicts.

Fixes

- Fixed an issue where an incorrect internal device event was triggered when presenting a credential at an NDE lock.
- Fixed an issue where hardware version was not displaying properly in the local panel admin interface (webcli).
- Fixed an issue where NDE locks with no credential entries in cache after being power cycled continued to allow card access.
- Fixed an issue where the ACS300 stated a door had closed when it was still in the process of closing.

Features

- This firmware release implements new event types for Wavelynx Bluetooth Readers.
- This firmware release allows the Allegion LE locks to operate in either persistent or non-persistent modes in regards to Privacy Mode.

Improvements

- When the server and panel disagree on a user's access for a swipe, the panel now automatically requests a fresh data file.
- The header under the Administration tab of the webCLI now more clearly states its purpose.
- Improvements to grammar were made under the OSDP Tool tab in the webCLI.
- Investigated and corrected startup errors in the ACS5000E panel logs.
- Brivo servers now update the panel local database immediately following an update to or deletion of user credentials.

Fixes

- Fixed an issue where panel could not process digital credential/BLE credential if the credential had not yet been cached.
- Fixed an issue where panels using the RS485 bus would not generate gateway communication events while the NDE gateway was without power.
- Fixed an issue where Allegion LE locks failed to operate after NDE gateway recovered from power failure and loss of network connectivity.
- Fixed an issue where expired credentials still worked when the panel was disconnected.
- Fixed an issue where loss of communication to an NDE gateway took too long to register in the Activity Log.
- Fixed an issue where Door Forced Open messages did not appear promptly after being triggered on ACS5000 and ACS-IDPC control panels.
- Corrected an issue with NDE Locks after power loss only sending a gateway communication restored message to the server when the panel is restarted without the accompanying communication lost message, which might have been confusing to some users.

Features

- This release implements CAN bus lockup detection logic as well as CAN bus recovery logic, allowing the control panel to detect an issue and then quickly resume normal operations after the recovery.

Fixes

- Fixed an issue where unexpected power failure caused database corruption and inability to recover.