RELEASE NOTES
BRIVO ONSITE SERVER 3.4.5.4
04/26/2019

This patch release of Brivo Onsite Server addresses system improvements and minor bug fixes.

Fixes

- Fixed an issue where credential holders were incorrectly identified as “Out of Effective Date Range” and denied access.
- Fixed a broken URL link for listing a filtered user page.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.5.3
04/04/2019

This patch release of Brivo Onsite Server primarily addresses issues experienced by some of our larger Brivo Onsite Server installations.

Improvements

- Upgraded to new Ethernet driver used by -A panels.
- Control panels are now able to receive panel data with credentials in pending states without Command Channel availability.
- Improved control panel SIGTERM recovery and restart logic.

Fixes

- Fixed a problem where door boards were appearing as I/O boards.
- Fixed an issue where custom fields were removed as a filter search option.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.5.2
02/17/2019

This patch release of Brivo Onsite Server primarily addresses memory issues with firmware upgrades with access control panels.

Improvements

- Improved ACS5000 panel firmware upgrade procedure to increase reliability.

Fixes

- Fixed a problem where an SQL error message improperly appeared in the Diagnostic Dump output from the system.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.5.1
01/24/2019

This patch release of Brivo Onsite Server primarily addresses reported issues of secure doors during panel daemon restarts.

Improvements

- Panel reboot now suppresses door forced and other hardware related events as a result of the paneld restart.
- Improved the speed of certain database queries.

Fixes

- Fixed a thread locking issue where Brivo Onsite Server where multiple work threads were working on the same task and producing multiple panel data sets for a single panel.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.5
12/21/2018

This release of Brivo Onsite Server adds Allegion AD400 Wireless Lock support as well as addressing system performance improvements and bug fixes.

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

- Administrator username and passwords in webCLI no longer allow ‘space’ or ‘#’ characters.
- Added detail memory usage for Brivo apps in the panel dump file.
- Increased Brivo Onsite Server system log size.
- New process doesn’t cause ACS5000 panels to run out of memory when using very large configuration files.
- Reduced unnecessary device status report messages causing server to run out of memory.

Fixes

- Fixed an ACS6000/ACS300 control panel memory leak.
- Fixed an issue causing panel logs to show ‘failed to sync hardware clock’ messages.
- Fixed CAN Bus kernel issue with backward compatibility with ACS6000 boards in the field.
- Fixed a reporting problem with communication between main boards and daughter boards.
- Added a watchdog mechanism for monitoring legacy panel command channel communications.
- Removed server side ethernet monitoring script causing false alarms.
- Added a watchdog mechanism for monitoring websocket traffic.
- Fixed an issue where DataSync was not properly returning External_IDs.
- Fixed an issue where system files were not being updated properly after system upgrade

---

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.4.4
10/31/2018

This release of Brivo Onsite Server addresses system performance improvements and bug fixes.

Improvements

- Panels no longer experience a processing slow down during threat level changes.

Fixes

- Fixed an issue where the Brivo Onsite Server appliance erroneously sent input switch device settings to control panels with no physical hardware.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.4.3
10/16/2018

This release of Brivo Onsite Server addresses system performance improvements and bug fixes.

Improvements

- Panels performing a controlled restart preserve the current state of all input and output relays.

Fixes

- Fixed an issue where a communication protocol (websocket) thread had become stuck with heavy network traffic. A watchdog was added to monitor the thread.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.4.2
09/10/2018

This release of Brivo Onsite Server adds the ability to enable or disable network monitoring from the webCLI as well as additional monitoring capabilities. Additionally, this release addresses system performance improvements and bug fixes.

Improvements

- Added the ability to enable or disable network monitoring from the webCLI.
- Added the control panel ID to the command channel log allowing for problems to be traced to specific panels when they occur.
- Erroneous door forced open messages and customer reported continuous relay clicking during panel restarts has been addressed by establishing proper timeout values for the command channel watchdog.

Fixes

- Fixed an issue where ACS6000/ACS300 panels using threat levels encountered problems on accounts with more than 160 schedules.
- Fixed a memory allocation issue affecting certain network environments.
- Fixed an issue where Exacq cameras were unable to display live view or recorded video.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.4.1
08/09/2018

This maintenance release of Brivo Onsite Server implements an improved queueing method for the command channel. Additionally, this release addresses system performance improvements and bug fixes.

Improvements

- Implemented new message queues for the command channel to help reduce delays. Command channel messages are now divided into high and low priority, ensuring high priority messages have the most timely processing.

Fixes

- Minor bug fixes.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.4
07/06/2018

This release of Brivo Onsite Server updates the Allegion LE lock functionality and implements new CAN bus logic for Brivo control panels. Additionally, this release addresses system performance improvements and bug fixes.

Features

- Administrative control now allows the Allegion LE button door lock to operate in both persistent or non-persistent modes with regards to privacy mode.

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.
- Updated confusing messaging to more clearly show that a fail-over from ethernet to WiFi has occurred and not just a communication failure.
- Corrected grammar on the OSDP Tool page of the webCLI.
- Changed the header on the webCLI Administrative Page to more clearly show both username and password.
- Improved the data channel failure retry mechanism.
- Updated the NTP client used for Brivo Onsite Server.
- Standardized the cache number for NDE cache size to allow entry of values (in multiples of 5) between 0 – 1275.
- Added backup NTP Server Address fields to prevent time-outs.

Fixes

- Fixed an issue where the webCLI was not properly displaying the hardware version.
- Fixed an issue where an incorrect internal device event was triggered when presenting a credential at an NDE lock.
- 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 io daemon generated transition states.
- Fixed an issue where the ACS300 io daemon was producing erroneous out of defined range messages.
- Fixed an issue where control panels using RS485 bus wouldn’t generate gateway communication events while the NDE gateway had lost power.
- Fixed an issue where power cycling an ACS300 caused loss or corruption of the panel configuration.
- Fixed an issue where Allegion LE locks failed to operate after the NDE gateway recovered from power failure and loss of network connectivity.
- Fixed an issue where slow door transitions on the door input resulted in erroneously door forced events.
- Fixed an issue where NDE gateways losing communication took 500 seconds to report.
- Fixed an issue with NDE locks always sending a gateway communication restored message when paneld restarts.

- Fixed an issue where the Brivo Onsite Server dashboard erroneously shows an occasional ACS6000 panel disconnect.
- Fixed an issue where Brivo Onsite Server generated duplicate event triggers when the event triggers are configured with a threat level.
- Fixed an issue where a door/device did not properly operate according to its assigned threat level.
- Fixed an issue where websocket command server would close the socket twice under certain conditions causing the command server to crash.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.3.1
03/19/2018

This maintenance release addresses bug fixes and other minor improvements to system performance.

Bug Fixes

- Corrected an issue with ACS300 panels where those panels were experiencing higher than expected Wiegand card read failures.
- Fixed an issue with ACS5000 and ACS-IPDC panels where Door Forced Open events did not appear in the Activity Log after a Door Forced event.
- Fixed an issue with ACS6000 and ACS300 panels where FIPS mode still showed OFF even when a panel was properly configured with a valid FIPS license.

RELEASE NOTES
BRIVO ONSITE SERVER 3.4.3
01/31/2018

This release improves the cybersecurity features of Brivo Onsite Server by updating the kernel to prevent side channel attacks (aka Spectre and Meltdown). Continuing with our efforts to improve end user security, the Admin Interface for control panels now allows administrators to configure their own user name and passwords. This release also introduces the ability to restart data or command channel services when the panel is experiencing difficulties. Additionally, this release addresses bug fixes and other minor improvements to system performance.

Features

- Brivo Onsite Server introduces the ability for administrators to reset panel communications through the System Tools interface. This action resets the panel communications for all panels connected to the Brivo Onsite Server appliance.
- Brivo Onsite Server introduces the ability for administrators to configure their own user names and passwords when configuring the webCLI admin interface.

Improvements

- This release updates the kernel of the Brivo Onsite Server software to prevent malicious attacks exploiting known processor flaws (aka Spectre or Meltdown).
- This release eliminates the Wireless tab from the Admin Interface on ACS5000 control panels when accessing the WebCLI. Wireless functionality is not available on ACS5000 control panels.
- Brivo Onsite Server provides the option to reduce repetitive postings concerning unauthorized IP access by our control panels.
- Brivo Onsite Server now provides improved logging information when a control panel is unable to retrieve a firmware update.

Bug Fixes

- Fixed an issue where a control panel connected to the Brivo Onsite Server appliance using the upgrade feature in the WebCLI admin interface did not properly detect invalid signatures in the upgrade file.
- Fixed an issue where the OSDP LED blink pattern displayed incorrectly during unlock schedules.
- Fixed an issue where a control panel loses its gateway and IP information when set to static parameters.
- Fixed an issue where event rate control settings were erased when a panel was reset.
- Fixed a spelling error found in panel logs.
- Fixed an incorrect status showing in the Brivo Onsite Server device status after removing an NDE gateway and locks.
- Fixed an issue where credential name was not matching the image displayed in the Swipe & Show tab on the Dashboard.

RELEASE NOTES
BRIVO ONSITE SERVER™ 3.4.2
12/01/2017

Expanding our integration with Allegion products, Brivo Onsite Server now includes Allegion LE lock support. Brivo also continues its dedication to improved panel security by introducing reporting features for unauthorized IP access by our control panels. If a Brivo control panel begins accessing IP addresses not approved by Brivo, an administrator can now be notified via email and through the activity log of the unauthorized access attempts. This release also introduces rate limiting (spamming filter) for tamper, wiring (I/O), and AC power lost/restored events, and the ACS6000 and ACS300 panels now list available SSIDs as part of Wi-Fi setup. Additionally, this release addresses bug fixes and other minor improvements to system performance.

Improvements

- Brivo Onsite Server now provides integration and support for Allegion LE locks.
- Brivo Onsite Server has introduced the capability to monitor outbound traffic and detect if IP addresses other than approved Brivo Host Addresses are being contacted. If an unknown (or unapproved) address is contacted, notifications can be created making the administrator aware of the unauthorized transmission.
- Brivo Onsite Server provides the option to reduce repetitive postings concerning tamper, wiring (I/O), and AC power lost/restored events by implementing the option to limit the number of times per minute such an event will be posted to the activity log or will trigger an email notification.
- Brivo Onsite Server provides a list of available SSIDs for ACS6000 and ACS300 panels when the administrator is choosing to connect to a wireless network.
- When handshaking a control panel with the Brivo Onsite Server, Brivo Onsite panels are now listed as an option in the dropdown list.

Bug Fixes

- Applied a critical security patch to WPA supplicant to address the Krack security vulnerability.
- Fixed an issue where Allegion NDE locks was sending duplicate door forced open events to the dashboard as well as an issue where start frame errors occurred during certain situations.
- Fixed an issue where OSDP readers show UTC instead of their designated timezone.
- Removed door board references in ACS300 panel information.
- Fixed an issue where Brivo Onsite Server was sending false unauthorized IP access alarms after a panel swap.
- Fixed an issue where input switch devices would not fire on ACS6000 and ACS300 when any delay duration was specified.
- Fixed an issue where the incorrect panel type was displayed when importing an ACS5000-S backup file.

- Fixed missing DNS configuration for Wi-Fi setup using static IP addresses.
- Fixed an issue where the data daemon crashed after restoring a backup file to the ACS6000 panel.
