Introducing the Exciting 4.3.1 Firmware Release for CHARGESTORM® CONNECTED 2

We are thrilled to announce the highly anticipated 4.3.1 firmware release for CHARGESTORM CONNECTED 2 (CC2). Packed with a multitude of new features, this update focuses on enhancing cyber security measures, ensuring a safer charging experience for both home and workplace charging in the UK and EU. Complying with the UK regulatory requirements on cyber security since January 1st, 2023, and aligning with the upcoming Radio Equipment Directive (RED) cyber security standards, this release sets a new standard for charging station security.

Let's delve into the exciting new features and improvements:

Enhanced Local Web Interface:

- Changeable Login Password: You now have the ability to change your login password easily. Furthermore, a convenient password reset button has been added to the top of the login page, ensuring you never lose access.
- Security Log: All security-related events, such as login attempts, are now logged in flash memory. You can download the log from the local Web UI to your connected computer. Additionally, the security log is automatically uploaded to the backend through the OCPP GetDiagnostics functions.
- Real-time Security Event Notification: Security events are instantly communicated to the backend via OCPP, providing you with real-time updates and ensuring prompt action.
- Tampering Detection: The software now supports tampering detection on the CCU R18 board. The tampering device can be enabled or disabled conveniently through a configuration parameter.

Comprehensive Cyber Security Improvements:

- Strengthened SSH Access: By default, SSH access to the charging station is disabled, enhancing overall security.
- Disabled Bootloader Debug Interface: Interrupting the boot process through the bootloader debug interface is no longer possible, ensuring uninterrupted operation.
- Hardened Firmware: All processes now run with minimal privileges, fortifying the system against potential vulnerabilities.
- Disabled Unused External Communication Interfaces: Any external communication interfaces that are not in use are now disabled, reducing potential attack vectors.
- Updated Linux/Yocto and QT: The firmware has been updated to the latest patch releases of Linux/Yocto, ensuring the inclusion of important security updates. Additionally, the firmware now utilizes the latest version of QT 6.2, which supports the most recent TLS version.

Bug Fixes for a Smooth Experience:

- Improved OCPP GetDiagnostics: The OCPP GetDiagnostics message now correctly handles the start and stop times, providing accurate diagnostic information.
- Responsive OCPP TriggerMessage: The response is now sent before taking action, ensuring efficient communication and synchronization.
- Fixed OCPP SendLocalList.conf Bug: A bug related to the OCPP SendLocalList.conf message has been resolved, eliminating any inconsistencies.
- Enhanced OCPP GetCompositeSchedule: While the OCPP GetCompositeSchedule is not implemented, the response to a request now accurately indicates that it is "not implemented."

Hardware Compatibility and Software Support:
The 4.3.1 release is compatible with the following CTEK EVSE units:

- All CC2 models
- CGC500
- CGC100 (Note: To upgrade to 4.3.1, the CGC100 requires the installation of the 3.18 release first.)

Please note that the 4.3.1 release is not compatible with CC1 models, as the CC1 CPU performance does not meet the requirements for this release. However, rest assured that CTEK will continue to support and maintain both the 3.x and 4.x software releases, ensuring seamless load balancing in installations where CC1 and CC2 coexist.

Identifying Your Device:
Determining whether you have a CC1 or CC2 model is easy:

- Check the article number on the CE label on the box. CC1 models always have "100" in the middle of the article number (###-100##).
- Alternatively, you can verify the model through the backend by checking the charge point model in the OCPP BootNotification message. The model name for CC1 is "Cs Connected v1," while CC2 is "Cs Connected v2."

Upgrade Information and Support:
Updating your Chargestorm Connected device to the 4.3.1 firmware is a breeze and comes at no additional cost. Simply follow the upgrade process, and you'll benefit from the latest features and enhanced security measures.

Important Reminders:

- Once a CC2 device is upgraded to 4.3.1, downgrading to a 3.x version is not possible.
- Please note that the 4.x releases are not compatible with CC1 models due to their limited CPU performance. Attempting to upgrade a CC1 to 4.3.1 will result in a failed update. Always ensure you verify your device model before proceeding with the firmware update.
- Load balancing functionality remains unchanged, allowing seamless operation in mixed installations of CC1 and CC2 devices.
- Our commitment to innovation and feature development primarily focuses on the 4.x releases. While there will still be 3.x releases, their main purpose will be to address bug fixes and ensure a smooth experience.

Join the Chargestorm Connected community and experience the enhanced capabilities and robust cyber security measures of the 4.3.1 firmware release. We're excited to empower you with a safer, more reliable, and efficient charging experience. Upgrade your device today and enjoy the benefits of our latest advancements, the firmware is available at https://www.ctek.com/uk/e-mobility-software

For any inquiries or assistance, our dedicated support team is here to help. Reach out to us with any questions or concerns you may have.

Thank you for choosing CHARGESTORM CONNECTED 2, where innovation meets security!