Выявленные уязвимости встроенного ПО УСПД СЕ805М:

Уязвимость: CWE-798: Use of Hard-coded Credentials; CWE-836: Use of Password Hash Instead of Password for Authentication

Описание: Возможность несанкционированного подключения и изменения настроек под пользователем SUPERVISOR

Уязвимость: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Описание: уязвимость в обработчике команды записи CMD_W_REG в регистр CEAR_MWDI_DFLT_PASSWORD, которая может привести к нарушению целостности БД или аварийному завершению исполняемого модуля.

Уязвимость: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CWE-94: Improper Control of Generation of Code ('Code Injection')

Описание: Команда записи CMD_W_REG регистра 0xCA протокола CE_A позволяет модифицировать SshUserPass параметр таким образом, чтобы выполнить вставку команд операционной системы, которые будут выполнены при запуске автообновления прикладного ПО.

Решение: Замена встроенного ПО на версию 4.13. Для получения обновления необходимо направить запрос на адрес: concern@energomera.ru