ИБ-эксперты нашли уязвимости в "умных" духовках AGA

Кен Мунро (Ken Munro), специалист по информационной безопасности (ИБ) британской компании Pen Test Partners (PTP), обнаружил уязвимости в новейших моделях духовых шкафов AGA iTotal Control. Как утверждает эксперт, воспользовавшись ими, злоумышленники могут с помощью простого СМС включить или выключить духовку.

Дело в том, что в AGA iTotal Control имеется SIM-карта для подключения к сотовой сети, благодаря чему "умной" духовке можно отправить текстовое сообщение с командой, по которой та включается или выключается. Сделать это можно непосредственно с мобильного телефона с помощью СМС, через приложение или с сайта производителя. По мнению ИБ-специалиста, эта функция является "слабым местом" прибора и представляет потенциальную угрозу для владельцев.

Также Мунро критикует производителя AGA за то, что удаленное управление духовкой тот организовал не через Wi-Fi-подключение, а с помощью модуля связи Tekelek и GSM SIM-карты EE, местного мобильного оператора. За возможность удалённо управлять кухонным прибором пользователю придется платить сотовому оператору по шесть фунтов стерлингов или свыше 420 рублей в месяц.

> "Выбранный AGA способ стоит около 70 фунтов в год и не подходит для районов с плохим уровнем сигнала сотовой связи", - констатирует специалист в своем блоге, выдержки из которого приводит издание The Register.

Для управления духовкой необходим телефонный номер, ассоциированный с SIM-картой прибора, однако AGA iTotal Control не делает никаких попыток проверить достоверность телефона, с которого приходит СМС. Этим недочётом вполне могут воспользоваться недоброжелатели. К примеру, послав духовке несанкционированную команду включиться, злоумышленник может "намотать" лишние киловатты энергии, или испортить ужин, если отключит прибор в неподходящее время.

Кроме того, Мунро выяснил, что подобрать номер SIM-карты духовки через веб-приложение производителя не составит большого труда. При введении неверных цифр выдается ошибка, но если номер верный, то появляется уведомление о том, что он уже зарегистрирован в системе. Путём перебора можно вычислить легитимный номер и отправлять духовке неавторизованные команды. Также оказалось, что на сайте используется незащищённое HTTP-подключение, а значит, хакеры могут перехватить трафик.

ИБ-специалисты Pen Test Partners попытались сообщить производителю о выявленных уязвимостях через Twitter и по электронной почте, однако так и не получили и от AGA никакого ответа. Впрочем, изданию в пресс-службе AGA заявили, что в курсе проблемы и уже ею занимаются.