Злоумышленники могут использовать SQL-инъекции для обхода авторизации и кражи данных.

Компания «Лаборатория Касперского» обнаружила 24 уязвимости в биометрических терминалах международного производителя ZKTeco. Эти бреши могут быть использованы злоумышленниками для обхода систем контроля доступа, физического проникновения в охраняемые зоны, кражи биометрических данных, внесения изменений в базы данных и установки бэкдоров.

Биометрические считыватели ZKTeco применяются в различных отраслях по всему миру, включая атомные электростанции, промышленные предприятия, офисы и учреждения здравоохранения. Они поддерживают четыре метода аутентификации: биометрический (с использованием распознавания лица), пароль, электронный пропуск и QR-код. В терминалах могут храниться биометрические данные тысяч людей. Все выявленные уязвимости были сгруппированы и зарегистрированы специалистами «Лаборатории Касперского», а информация о них была передана производителю.

Одной из уязвимостей (CVE-2023-3938) можно воспользоваться для получения физического доступа к закрытым зонам. Она связана с возможностью проведения кибератак на основе SQL-инъекции, что позволяет злоумышленникам внедрить вредоносные данные в QR-код. При обработке такого запроса система ошибочно распознает его как исходящий от легитимного пользователя, что позволяет получить несанкционированный доступ к терминалу и, соответственно, к охраняемым зонам.

В компании рассказали, что существует и другая возможность обмана системы. Если злоумышленник получит доступ к базе данных устройства, он может скачать фотографию легитимного пользователя, распечатать её и использовать для обмана камеры терминала. Однако для успешной реализации этого метода необходимо отключить тепловые датчики на устройстве.

Другая группа уязвимостей (CVE-2023-3940) позволяет злоумышленникам получать доступ к любому файлу в системе, включая конфиденциальные биометрические данные и хэши паролей, что может привести к компрометации корпоративных учетных данных. Однако интерпретация украденных биометрических данных представляет значительную сложность.

Ещё одна уязвимость (CVE-2023-3941) даёт возможность злоумышленникам вносить изменения в базу данных устройства, например, загружать собственные фотографии и

добавлять себя в список авторизованных пользователей. Кроме того, эта уязвимость позволяет заменять исполняемые файлы, что делает возможной установку бэкдоров.

Две другие уязвимости (CVE-2023-3939 и CVE-2023-3943) позволяют выполнять произвольные команды или код на устройстве, предоставляя злоумышленникам полный контроль с высшим уровнем привилегий. Это создаёт угрозу для всей корпоративной инфраструктуры, так как устройство может быть использовано для атак на другие сетевые узлы.