УДК004.416.6

МОБІЛЬНІ ДОДАТКИ ДЛЯ АСУ ТП УРАЗЛИВІ

Мирончук К.П, студент групи ІБ-41
Вацлавик О.М., викладач кафедри УІБ,
Львівський державний університет безпеки життєдіяльності

Більша половинапрограмних продуктів не захищена від злому і «лівої» авторизації. Дослідження стосувалося 34 програмних продуктів 20 вендорів, які призначені для збору, обробки, відображення та архівування інформації про об'єкти автоматизованих систем управління технологічними процесами.

Додатки, які є в магазині GooglePlay і зазвичай встановлюються інженерами на планшетах. Програма взаємодіє безпосередньо до об'єктів управління через Bluetooth, Wi-Fi; віддалене підключення можливо через Інтернет і мобільні мережі.

В цілому у 34 додатків знайдено 140 вразливостей. Тільки два з аналізованих додатки захищені від злому; на другому місці (59%) - небезпечна авторизація; на третьому (53%) - відсутність кодів і інших механізмів, призначених для запобігання зворотного проектування.

Більшість з них - логічні і архітектурні, і експлуатувати їх досить просто. Серед виявлених вразливостей: незахищені або недостатньо захищені методи передачі і зберігання даних (в тому числі, некоректне використання SSL або «саморобні» криптоалгоритми), віддалена атака на відмову в доступі на клієнт і сервер, SQL-ін'єкції, використання недовірених вхідних даних в якості параметрів настройки техпроцесу і ін. Особливу тривогу викликає той факт, що в додатках віддаленого доступу було знайдено більше вразливостей і слабкостей, ніж в клієнтах для роботи всередині безпечного периметра. Це неприпустимо для рішень, які працюють через незахищені канали зв'язку.

Експлуатація перерахованих проблем ІБ потенційно дозволяє реалізувати ряд небезпечних атак як на додаток, так і на оператора. В останньому випадку, реально створити хибне уявлення про поточний стан технологічного процесу, що може призвести до прийняття неправильних рішень з важкими наслідками для підприємства.

Метою дослідження в рамках даної роботи було не тільки знайти помилки безпеки в мобільних додатках для АСУ ТП, а й спробувати екстраполювати ризики компрометації цих додатків на ризики компрометації всієї інфраструктури АСУ ТП. Цей підхід відрізняється від звичного погляду на оцінку безпеки мобільних додатків: уразливості з традиційно низьким рівнем небезпеки можуть піддати АСУ ТП величезному ризику, а уразливості, які зазвичай вважаються критичними загрозами, навпаки, бувають небезпечні для АСУ ТП з дуже низькою ймовірністю.

Багато додатків не здатні безпечно зберігати і передавати дані. Майже половина протестованих додатків також не змогла безпечно зберігати дані. Дані часто зберігаються на SD-карті або віртуальному розділі, і вони не захищені списками управління доступом або іншими механізмами вирішення.

Тож не дивно, що більше третини проаналізованих додатків не змогли захистити зв'язок, в тому числі за допомогою взаємного посвідчення авторства і цілісності, неправильних версій SSL і передачі даних з відкритим текстом.

Це стосується клієнтської функціональності. Що стосується проблем зв'язку з серверної частиною, дослідники виявили різні типи вразливостей, включаючи SQL-ін'єкції, пошкодження пам'яті, DoS і витік інформації.

Резюмуючи висновки, можна сказати, що ситуація в області захищеності мобільних клієнтів для АСУ ТП досить важка. Якість коду в таких рішеннях дуже низька, зустрічаються воістину курйозні помилки і уразливості. Можливо, це пов'язано з тим, що область АСУ ТП дуже специфічна, і розробники мобільних рішень просто не віддають собі звіту в тому, що відбувається. Однак, такий стан справ є неприпустимим для сфери критично важливих об'єктів. І чим швидше фахівці усвідомлюють рівень небезпеки, тим краще.

ЛІТЕРАТУРА

1. Мобільна безпека [Електронний ресурс]– Режим доступу: 1wr / category / mobilnaya_bezopasnost / mobilnaya_bezopasnost / 1, вільний;

2. Безкоровайний Д. Безпека мобільних пристроїв // Відкриті системи СУБД, М: Видавництво «Відкриті системи», 2011. -26 с.

3. Вплив мобільних пристроїв на безпеку інформації [Електронний ресурс]– Режим доступу http: // www. anti-malware. ru /, вільний;