АНАЛИЗ УЯЗВИМОСТЕЙ ПРЕДУСТАНОВЛЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОБОРУДОВАНИЯ КАТЕГОРИИ «УМНЫЙ ДОМ»

Р.Е. Данилин, А.В. Мансуров
Алтайский государственный университет, г. Барнаул

В последнее время устройства категории «Умный дом» становятся все более популярны, разработкой подобных технологий занимается огромное количество компаний, на рынке постоянно появляются новые решения и их реализации: smart tv, умные кофеварки, электронные замки, различные типы датчиков, розетки с возможностью удаленного управления, системы домашней безопасности и т.д. Подобные устройства имеют различные средства аудио и видео фиксации, системы распознавания голоса и лица, возможность самостоятельного функционирования и функционирования в качестве элемента системы. На данный момент проводится проектирование подобных систем на уровне городов, например, программа «Безопасный город» [1] - это комплекс программно-аппаратных средств и организационных мер для обеспечения видеоохраны и технической безопасности, а также для управления в едином информационном пространстве объектами жилищно-коммунального хозяйства и другими распределёнными объектами. Учитывая темпы роста данной сферы рынка, многие производители, в стремлении занять определённую нишу, отодвигают безопасность производимых устройств на второй план. Все вышеперечисленные факты характеризуют подобные устройства, как потенциальный канал утечки большого количества конфиденциальной информации. Что делает их привлекательными для злоумышленников различной квалификации и создает необходимость непрерывного процесса поиска уязвимостей, а также их своевременного исправления.

Наиболее интересными для злоумышленника являются центральные управляющие устройства инфраструктуры умного дома т.к. они позволяют получить полный контроль над всей системой. В качестве объектов исследования были выбраны четыре управляющих блока (координатора) из различных ценовых сегментов. Например, подобные устройства производят Embedded Systems, ABB, Fibaro и Dlink. Данное оборудование устанавливается на границе сети умного дома и предоставляет возможность удаленного управления.

В общем случае исследование на наличие уязвимостей предустановленного программного обеспечения включает в себя следующие этапы:

- Получение образа прошивки устройства.
- Анализ сжатия и способа упаковки файла
- Идентификация архитектуры процессора
- Нейтрализация обфускации и распаковка образа
- Монтирование файловой системы устройства
- Проведение реверс – инжиниринга файла исходного кода
- Анализ полученных данных на наличие уязвимостей и недокументированных возможностей.

При успешном выполнении этапов, перечисленных выше, для анализа становятся доступны декомпилированный исходный код операционной системы одного из устройств и ряд конфигурационных файлов, в которых могут быть найдены различные недокументированные возможности, уязвимые сервисы, различные закладки от производителя и т.д. В выбранных для исследования устройствах (конкретное наименование устройства и производителя не приводится по этическим соображениям) был найден ряд тонких мест, имеющих критическое значение для общей безопасности оборудования, наиболее опасные из них рассмотрены в этой статье.

Управляющий блок №1. В ходе анализа исходного кода операционной системы было выяснено, что в устройстве по умолчанию активирован протокол управления SNMP второй версии [4]. Он имеет ряд концептуальных уязвимостей, однако поддержка более новых версий протокола устройством не предусмотрена. В случае попадания злоумышленника в сеть данная проблема безопасности позволит ему захватить полный контроль над устройством управления умным домом. Также был обнаружен включенный по умолчанию устаревший протокол поточного шифрования – RC4. Несмотря на поддержку устройством более криптостойких алгоритмов шифрования, этот параметр позволяет злоумышленнику производить попытки принудительной авторизации по наименее защищенному протоколу или перехватывать данные по средствам MITM атак.

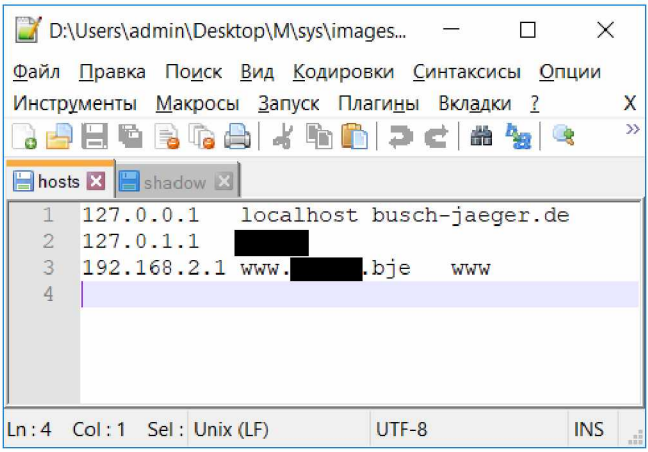
Управляющий блок №2. В ходе анализа конфигурационных файлов была обнаружена часть базы данных (Lili.sql), содержащая ряд служебных пользователей с указанием групп к которым они относятся:

INSERT INTO "Lili_Tokens" ("Token_Group", "Text", "Lang") VALUES ('all', 'everywhere', 'en');

INSERT INTO "Lili_Tokens" ("Token_Group", "Text", "Lang") VALUES ('all', 'both', 'en');

Это позволяет злоумышленнику сократить время на проведение атаки типа брутфорс – нет необходимости проверять существующих пользователей, остается подобрать только пароль для получения доступа к базе данных. Исследуемое устройство содержит встроенный сервер телефонии Asterisk. Пароль администратора телефонии хранится в открытом виде, что позволяет злоумышленнику получить контроль над всеми входящими и исходящими соединениями АТС.

Управляющий блок №3. На исследуемом устройстве некорректно реализован процесс обновления программной составляющей (рисунок). В данном устройстве отсутствует проверка подписи при установке программного обеспечения, и оборудование сконфигурировано таким образом, что сервер обновлений должен находиться по адресу в локальной сети. Это позволяет злоумышленнику поставить себя на место сервера обновлений и исполнить произвольный код на атакуемом устройстве.



Содержание файла images\root\etc\hosts

Управляющий блок №4. В ходе анализа было обнаружено, что обработкой Web-запросов занимается CGI-приложение web_cgi.cgi. Обработкой запросов HNAP занимается функция do_hnap в

web_cgi.cgi. Т.к. HNAP-действия посылаются как HTTP POST-запросы, функция do_hnap сначала обрабатывает заголовок Content-Length. Далее, происходит чтение и запись запроса в буфер фиксированного размера на стеке. Наиболее критичным в данном случае является то, что обработчик читает тело POST-запроса в буфер в цикле с использованием fgetc, поэтому не существует «плохих» байт — значит, в качестве запроса можно передавать любые данные, даже NULL-байт. Это облегчает процедуру переполнения стека злоумышленником с последующим захватом управления.

Результаты исследования демонстрируют тот факт, что к выбору оборудования категории «Умный дом» необходимо подходить с большой осторожностью, даже устройства верхнего ценового сегмента подвержены критическим уязвимостям. Системы подобного рода нуждаются в квалифицированной и гибкой настройке с точки зрения безопасности. Они должны быть выделены в отдельный сегмент от основной домашней сети и осуществлять удаленное взаимодействие с пользователем только по шифрованному каналу. В противном случае система станет постоянным источником утечки конфиденциальной информации.

Библиографический список.

1. Что такое программа «Безопасный город»? // ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ ПО АЛТАЙСКОМУ КРАЮ [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://22.xn--b1aew.xn--p1ai/citizens/faq/133. – Загл. с экрана.
2. Лав Р. Разработка ядра Linux. М. : ООО "И. Д. Вильямс", 2008. – 448 с.
3. Таненбаум Э., Вудхалл А. Операционные системы. СПб. : Питер, 2007. – 704 с.
4. Уязвимые места в SNMP // Открытые системы [Электронный ресурс]. – Электрон. ресурс. – Режим доступа : http://www.osp.ru/os/2002/12/182237/. – Загл. с экрана.