ПРОБЛЕМА БЕЗОПАСНОСТИ СМАРТ-КОМПОНЕНТОВ СИСТЕМЫ УМНОГО ДОМА

Кункевич Д.С.

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Скудняков Ю.А.- доцент каф. ПЭ, к.т.н,, доцент

Приводится описание уязвимости IoT-устройств.

По всему миру уже установлено огромное множество устройств, подключенных к Интернету, от датчиков до детских игрушек. Умный дом становится дешевле - им стало проще управлять. Сегодня пользователю не нужно иметь дело с несколькими приложениями для каждого устройства: посредством «умных помощников» он может пользоваться всем и сразу. При этом ведущие специалисты считают, что когда дело касается интернет-технологий, умеренный уровень паранойи вполне уместен.

В рамках презентации на конференции S4x19 команда специалистов из компании ForeScout раскрыла подробности об уязвимостях в протоколах и компонентах систем автоматизации «умных» зданий, предоставляющих широкие возможности для кибератак. В общей сложности исследователи обнаружили шесть проблем, в том числе XSS-уязвимости, уязвимости обхода каталога и обхода аутентификации, с помощью которых злоумышленник мог бы похитить конфиденциальную информацию, получить доступ и удалить критические файлы, а также производить другие вредоносные действия [1].

С целью демонстрации рисков современных «умных» зданий специалисты разработали вредоносное ПО, атакующее системы управления доступом, видеонаблюдения, отопления, вентиляции и кондиционирования и протестировали его в лабораторных условиях. Как правило, сеть САЗ (система автоматизации зданий) состоит из различных компонентов (системы отопления, вентиляции и кондиционирования, видеонаблюдения, диспетчерский контроль состояния оборудования электрощитовых, лифтов, сигналов от систем пожарной сигнализации и пр.). Подобная инфраструктура присутствует не только в жилых и коммерческих зданиях, но и в больницах, аэропортах, школах, дата-центрах и т.д. Эксперты обнаружили три XSS-уязвимости в контроллере управления доступом и протоколе шлюза, позволяющих внедрить вредоносные скрипты в web-интерфейс уязвимого устройства и получить cookie-файлы и идентификаторы сессии. В ПЛК также были обнаружены уязвимость переполнения буфера и вшитый пароль.

В протоколе шлюза содержались уязвимости обхода каталога и удаления файлов, предоставляющие доступ к папкам и файлам работающего на уязвимом устройстве web-приложения. Еще одна проблема присутствовала в контроллере управления системой отопления, вентиляции и кондиционирования. Она позволяла обойти механизм аутентификации и украсть учетные данные пользователей, включая «хранимые в открытом виде пароли». Информация о всех уязвимостях была передана производителям уязвимых систем, которые уже выпустили соответствующие патчи.

Согласно результатам поиска Shodan и Censys, из 22 902 публично доступных устройств (в том числе IP-камер) более 9 тыс. были подвержены указанным уязвимостям. Ситуация с камерами видеонаблюдения значительно хуже – 91% (10 312) из обнаруженных 11 269 устройств оказались уязвимыми. По словам специалистов, вредоносные программы для атак на САЗ могут использовать четыре вектора – общедоступные ПЛК, управляющие приводами и датчиками; уязвимые рабочие станции для управления всей системой; публично доступные IoT-устройства (камеры наблюдения или маршрутизаторы), физически изолированные сети (для проникновения в сеть потребуется физический доступ). *На многих бытовых смарт-устройствах включены устаревшие версии UPnP.*

Ранее неизвестные засыпали пользователей Chromecast, Google Home и смарт-телевизоров спам-сообщениями с призывом подписаться на YouTube-канал видеоблогера Pew Die Pie. Согласно отчету исследователей Trend Micro, спамеры, очевидно, воспользовались некорректной конфигурацией маршрутизаторов с включенным сервисом Universal Plug and Play (UPnP).

Многие устройства «интернета вещей» (IoT) используют UPnP для автоматического обнаружения, проверки и связи с другими устройствами в одной с ними локальной сети. UPnP существенно упрощает жизнь, но в то же время добавляет дополнительные угрозы безопасности. С помощью бесплатных инструментов для сканирования IoT-устройств исследователи Trend Micro обнаружили, что на гаджетах пользователей по-прежнему активирован UPnP. По состоянию на январь 2019 года сервис был включен на 76% маршрутизаторов, 27% медиа-устройств (DVD-проигрывателях, стриминговых устройств и пр.) и 19% игровых консолей. Злоумышленники могут превратить уязвимые реализации UPnP в прокси для обфускации ботнетов, а также в ботов для осуществления DDoS-атак и рассылки спама. Ярким примером является ботнет Satori, операторы которого эксплуатируют уязвимость в Realtek SDK miniigd, использующемся в интерфейсе UPnP SOAP (CVE-2014-8361). Уязвимость, позволяющая внедрять команды, была исправлена в мае 2015 года, однако на многих устройствах по-прежнему используются устаревшие уязвимые версии UPnP.

Список использованных источников:

1. Security lab [электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/tags/IoT/ – Дата доступа: 10.03.2019.