Анлим

Аналитический отчет

по найденным потенциальным уязвимостям и факторам, снижающих защищенность информации

14.05.2020г

Настоящий Отчет содержит анонимные статистические данные об анализе используемых в рамках работы сайтов служб и найденных сведений о потенциальных уязвимостях. Вся информация была получена с помощью публичных, открытых источников и без активного взаимодействия с сайтами.

Специалистами компании проанализировано 129 сайтов, из которых в отношении 64 были найдены сведения о наличии потенциальных уязвимостей.

Ниже представлен график, отражающий количественное распределение найденных в ходе анализа сайтов и сервисов потенциальных уязвимостей и факторов, снижающих уровень защищенности информации *(см. график 1).*

График 1. Потенциальные уязвимости и факторы, снижающие защищенность информации

На первом месте по распространенности – наличие общеизвестных уязвимостей, которым присвоен уникальный идентификатор (CVE). В ходе анализа выявлено 45 сайтов с потенциальными уязвимостями, которым присвоен идентификатор CVE. Более развернутая по составу выявленных уязвимостей информация приведена далее (см. график 2).

Один из возможных векторов атаки, связанный с использованием таких уязвимостей: злоумышленник получает удаленный доступ к сервису, проводит повышение прав доступа до администратора системы и получает полный контроль над узлом. Дальнейшие действия ограничиваются только его фантазией: от компрометации базы данных и до искажения ресурса.

На втором месте – утечка паролей от корпоративных почтовых ящиков сотрудников. Для 34 сайтов были найдены сведения о ранее скомпрометированных паролях от корпоративных почтовых ящиков сотрудников. Используя такие данные, злоумышленник может попытаться войти в иные сервисы и системы с идентичными или схожими по «маске» паролями. В первую очередь это актуально для корпоративных ресурсов организации и может привести к краже данных клиентов или нарушению нормального функционирования сервиса. Также возникает вероятность рассылки фишинговых писем с скомпрометированных почтовых адресов организации, что может повлечь возникновение репутационных рисков.

На третьем месте – возможность обращения к СУБД из публичной сети Интернет. Указанный факт расширяет потенциальную поверхность атаки для злоумышленника и повышает вероятность получения несанкционированного доступа к информации, хранящейся в базах данных, например, к персональным данным сотрудников, клиентов или партнеров. У 20 организаций СУБД доступна из публичной сети.

На четвертом месте – сайты, которые используют протокол HTTP, то есть передача данных осуществляется без шифрования. Выявлено 15 сайтов, использующих незащищенный шифрованием протокол. Такие сайты подвержены перехвату пользовательских данных (логин, пароль, сессия и др.), так как информация передается открытым текстом, без шифрования.

На пятом месте – компрометация паролей от личных почтовых ящиков сотрудников. Использование указанного фактора злоумышленником может привести к возможности доступа к ресурсу аналогично компрометации корпоративной почты, а также послужить одним из этапов действий злоумышленника по компрометации корпоративной почты сотрудника. Скомпрометированные пароли выявлены в отношении лиц, аффилированных с 14 компаниями.

На шестом месте – сайты, размещенные на собственных серверах организаций. Выявлено 13 таких сайтов, 6 из которых имеют потенциальные уязвимости по классификатору CVE. При обнаружении связки «собственный сервер плюс потенциальные уязвимости по классификатору CVE», злоумышленник, получив контроль над сайтом, возникает риск получения доступа до других объектов в локальных сетях организации и компрометации иных информационных ресурсов.

На седьмом месте – открытая конфигурация. При разработке сайтов и сервисов часть кода, код целиком или файлы конфигураций разработчики хранят на сторонних сервисах, для удобства работы, и после завершения разработки не удаляют информацию, в результате она становится общедоступной. Данная информация может быть очень полезна для злоумышленника, например, для определения версий технологий, используемых на сервере, поиска под выявленные версии эксплоитов в открытом доступе и вычисления других слабых мест. Такая информация была найдена в отношении 8 сайтов.

На восьмом месте – сайты, вход в панель управления которых основан на Basic Authentication. Это технология устарела и имеет ряд уязвимостей на уровне архитектуры, например, логин и пароль от клиента к серверу передаются в открытом виде и подвержены перехвату злоумышленником. Кроме того, данная технология не защищена от перебора логина и пароля «по словарю», что позволит злоумышленнику за некоторое время определить корректные учетные данные. Basic Authentication до сих пор используется на 5 сайтах.

На девятом месте – открытые контакты сотрудников. Ряд организаций хранят на своих сайтах справочники с данными сотрудников, в которых указаны ФИО, должность, телефон и, иногда, домашний адрес. Такая информация может быть полезна злоумышленнику, например, для подготовки к фишингу или применению методов социальной инженерии. Указанные справочники обнаружены на 4 сайтах.

Для наглядности выявленные потенциальные уязвимости с присвоенными идентификаторами CVE отсортированы по частоте выявления *(см. график 2)*.

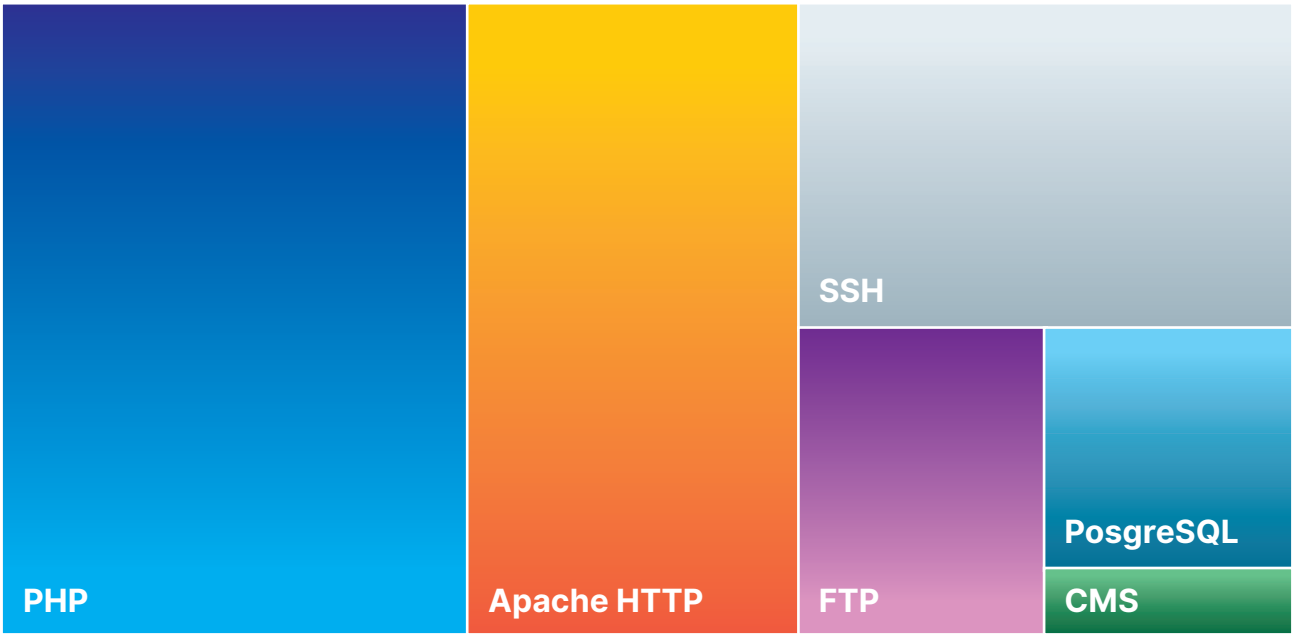

График 2. CVE

Самыми распространёнными оказались уязвимости, связанные с PHP, Apache и SSH.

Уязвимости протокола SSH, в основном, позволяют определить существующих пользователей системы.

Более половины уязвимостей с идентификаторами CVE на PHP, Apache, FTP, PostgreSQL позволяют злоумышленнику провести атаку типа «отказ в обслуживании».

На одном из исследуемых сайтов выявлена потенциальная уязвимость в CMS позволяющая получить доступ к панели управления сервисом.

С общеизвестными уязвимостями, которым присвоен уникальный идентификатор (CVE), выявлено 45 компаний. Для исправления большинства данных уязвимостей требуется обновить версию программного обеспечения до актуальной. Вендоры в подавляющем большинстве своевременно выпускают обновления, но как показывает статистика выше, а также опыт проведения тестирования иных сервисов и систем, не каждый системный администратор их устанавливает.

Самой распространенной ошибкой по сей день остаются слабые и повторяющиеся пароли. В совокупности, скомпрометированные пароли выявлены от личных и (или) корпоративных почтовых ящиков лиц, связанных с 48 компаниями. Согласно опросу Avast, 55% российских пользователей используют одинаковые пароли для разных аккаунтов, хотя 94% знают, что это опасно.