УДК 004.492.2

Степичев А.С.,
студент магистратуры
1 курс, факультет «Институт магистратуры»
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Россия, г. Санкт-Петербург
Научный руководитель: Кушнир Д.В.

СКАНИРОВАНИЕ ПК НА НАЛИЧИЕ УЯЗВИМОСТЕЙ В СИСТЕМЕ БЕЗОПАСНОСТИ И УСТРАНЕНИЕ ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ ПРИ ПОМОЩИ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ SCANOVAL

Аннотация: *Статья посвящена поиску и устранению уязвимостей в системе безопасности компьютера посредством бесплатного ПО ScanOVAL. В данной статье содержится информация о том, что такое уязвимость программ и опасность их наличия. Также рассматривается пример устранения выявленных уязвимостей.*

Ключевые слова: *система безопасности, уязвимость, программное обеспечение, ScanOVAL, уровень угрозы.*

Abstract: *The article is devoted to the search and elimination of vulnerabilities in the computer security system using the free ScanOVAL software. This article provides information on what software vulnerabilities are and the danger of their presence. An example of eliminating identified vulnerabilities is also considered.*

Key words: *security system, vulnerability, software, ScanOVAL, severity rating.*

Введение

В наше время информационные технологии используются повсеместно, и многие уже не могут представить свою жизнь без них: социальные сети, онлайн-банкинг, интернет-магазины — все это стало частью нашей жизни, но все точки доступа к этим ресурсам потенциально уязвимы. Именно поэтому информационная безопасность, в современных реалиях, играет крайне важную роль в нашей жизни. Так же, стоит отметить, что защита личных данных перманентно усложняется в следствие развития технологий. В данной статье я хотел бы рассмотреть механизм обнаружения уязвимостей в безопасности при помощи ПО ScanOVAL и их последующего устранения.

Уязвимости в системах безопасности и необходимость в их устранении

Уязвимостями программ называются ошибки, допущенные программистами во время разработки программного обеспечения. Наличие уязвимостей позволяет злоумышленникам получить незаконный доступ к функционалу программы и данным хранящимся в ней. Изъяны могут проявиться на любом этапе жизненного цикла ПО, с начала проектирования и вплоть до выпуска готового продукта. Иногда программисты нарочно оставляют лазейки в своих программах для проведения отладки и настройки. Подобные приемы также могут рассматриваться в качестве бекдоров или недекларированных возможностей.

В массе случаев возникновение уязвимостей обусловлено использованием средств разработки различного происхождения, которые повышают риск появления в программном коде дефектов диверсионного типа.

Как уже было сказано, уязвимости возникают в результате просчетов, возникших на этапе проектирования или написания программного кода.

В зависимости от стадии появления, угрозы делится на уязвимости проектирования, реализации и конфигурации.

- Ошибки, допущенные на этапе проектирования, самые сложные для обнаружения и устранения. К ним относятся неточности алгоритмов, несогласованности в интерфейсе между различными модулями или в протоколах взаимодействия с аппаратной частью, введение неоптимальных технологий. Их устранение является очень трудоемким процессом, так как они могут проявиться в весьма неочевидных случаях — к примеру, при превышении предусмотренного объема трафика или при избыточном подключении дополнительного оборудования. Подобные моменты усложняют обеспечение требуемого уровня безопасности и приводит к возникновению путей обхода межсетевого экрана.
- Уязвимости реализации возникают на этапе написания программного обеспечения или внедрения в него алгоритмов безопасности. К ним относятся некорректная организация вычислительного процесса, логические и синтаксические дефекты. При этом существует риск, что данного рода изъян приведет к переполнению буфера или появлению неполадок иного рода. Их обнаружение занимает много времени, а устранение подразумевает исправление определенных фрагментов машинного кода.
- Ошибки конфигурации аппаратной части и программного обеспечения встречаются довольно часто. Наиболее распространенными причинами их возникновения могут быть недостаточно качественная разработка и отсутствие тестов на корректность работы дополнительных функций. К данной категории также можно отнести слишком простые пароли и, оставленные без изменений, данные учетной записи.

По статистике, чаще всего уязвимости выявляются в популярных и распространенных продуктах — десктопных и мобильных ОС, браузерах.

Программы, в которых обнаруживают наибольшее число уязвимостей, распространены практически на всех компьютерах. Киберпреступников напрямую заинтересованы в поиске подобных изъянов и написании различных эксплойтов под них. Ввиду того, что с момента обнаружения уязвимости до

выпуска патча (исправления) проходит немало времени, существует внушительное количество возможностей заразить системы компьютера через дыры в безопасности программного кода. При этом достаточно будет того, чтобы пользователь ПК только один раз открыл, например, вредоносный PDF-файл с эксплойтом, после чего хакеры получат доступ к данным на его компьютере. Заражение в данном случае происходит согласно следующему алгоритму:

- Пользователю по электронной почте приходит фишинговое письмо от доверенного отправителя.
- К письму прикреплен файл с эксплойтом.
- Как только пользователь пытается открыть файл, происходит заражение компьютера вирусом, трояном или другой вредоносной программой.
- Злоумышленники заполучают несанкционированный доступ к системе, с последующей возможностью кражи ценных данных.

Краткая характеристика программы ScanOVAL

Программное обеспечение ScanOVAL выполнение следующих основных функций:

- загрузка XML-файлов с OVAL-описаниями уязвимостей, выполненными в соответствии со стандартом «The OVAL Language Specification» версии не ниже 5.10.1;
- обработка данных и обнаружение, представленных в XML-файлах, уязвимостей программного обеспечения, установленного на локальной ПЭВМ, работающей под управлением операционной системы семейства Microsoft Windows.

Программное обеспечение ScanOVAL функционирует под управлением операционных систем Microsoft Windows 7/8/8.1/10 или серверных операционных систем Microsoft Windows Server 2008/2008R2/2012/2012R2/2016.

Для обеспечения работы программы ScanOVAL потребуется следующее программное обеспечение:

- Microsoft .NET Framework версии не ниже 4.0;
- интерпретатор языка OVAL 5.10.1 или выше (предоставляется совместно с дистрибутивом ScanOVAL).

Сканирование домашнего ПК посредством ПО ScanOVAL

В результате сканирования домашнего ПК было выявлено 19 уязвимостей, представленных на рисунке 1. Из них:

- 1 с НИЗКИМ уровнем угрозы (0,0…3,9 по шкале CVSS)
- 9 со СРЕДНИМ уровнем угрозы (4,0…6,9)
- 9 с ВЫСОКИМ уровнем угрозы (7,0…9,9)

Уязвимостей с КРИТИЧЕСКИМ уровнем опасности обнаружено не было.

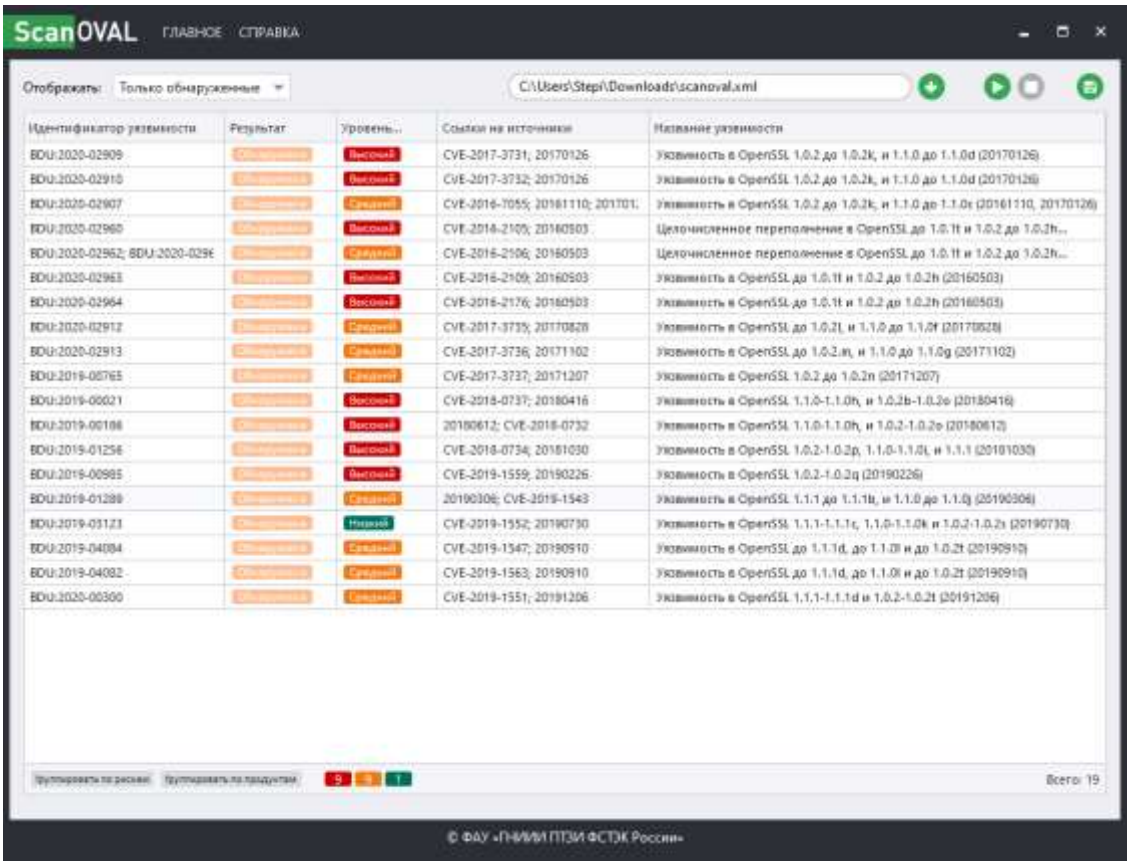

Рисунок 1. Уязвимости выявленные на домашнем ПК

Устранение обнаруженной уязвимости

Операции устранения была подвержена уязвимость с идентификатором BDU:2020-02964, имеющая ВЫСОКИЙ уровень угрозы. Данная уязвимость имеет следующее описание:

Функция X509_NAME_oneline в crypto/x509/x509_obj.c в OpenSSL до 1.0.1t и 1.0.2 до 1.0.2h позволяет удалённым злоумышленникам получить доступ к конфиденциальной информации через память стека процесса и вызвать отказ в обслуживании (чтение за пределами буфера) через специально сформированные EBCDIC ASN.1 данные.

Рисунок 2. Описание устраняемой уязвимости

Согласно описанию, источником уязвимости является библиотека ssleay32.dll. Программа ScanOVAL в качестве решения предлагает обновить криптографическую библиотеку OpenSSL до версии 1.0.2h и новее.

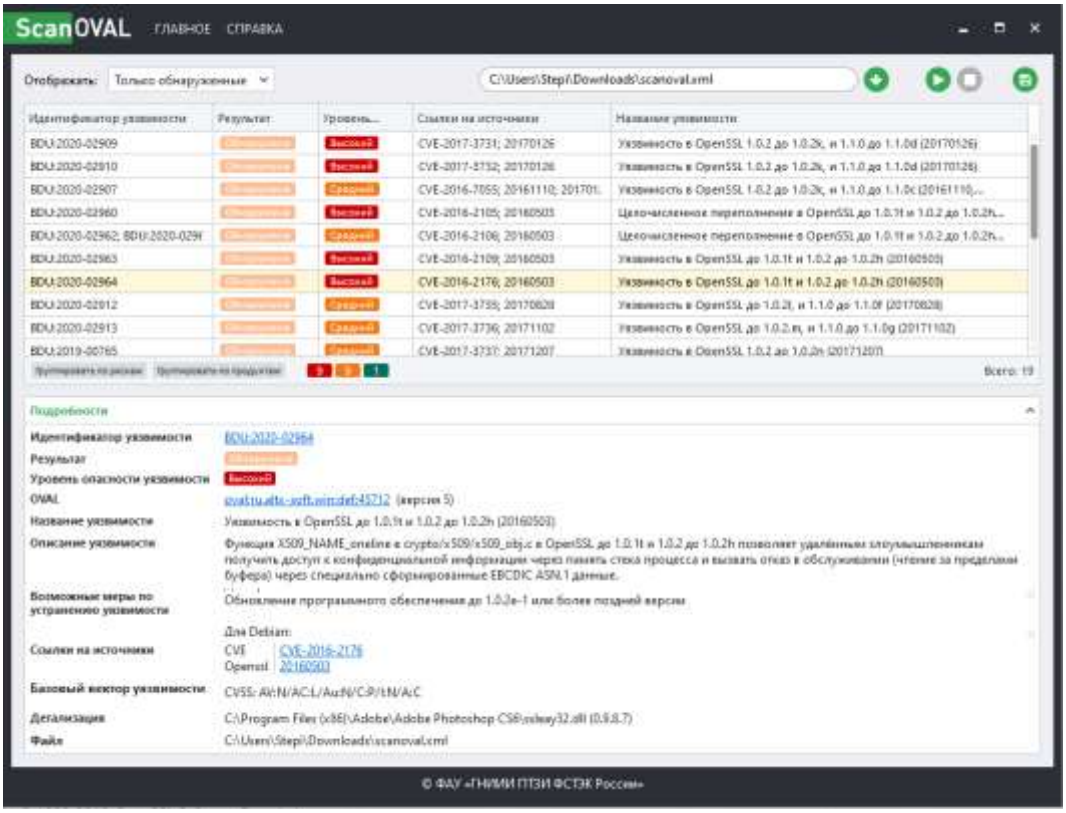

Рисунок 3. Подробности об устраняемой уязвимости

Обновляем OpenSSL до самой новой версии 1.1.1h. Следующим шагом копируем обновленную библиотеку ssleay32.dll по адресу, указанному в отчете ScanOVAL (C:\Program Files (x86)\Adobe\Adobe Photoshop CS6\ssleay32.dll).

Результаты выполненной работы

После вышеописанных действий проводим сканирование на наличие уязвимостей заново. В результате повторного сканирования обнаруживаем, что нам удалось избавиться не только от преследуемой уязвимости, но и еще от 2 уязвимостей с ВЫСОКИМ уровнем угрозы и 1 с СРЕДНИМ (Пропали уязвимости со следующими идентификаторами: BDU:2020-02960, BDU:2020-02962, BDU:2020-02963 и BDU:2020-02964).

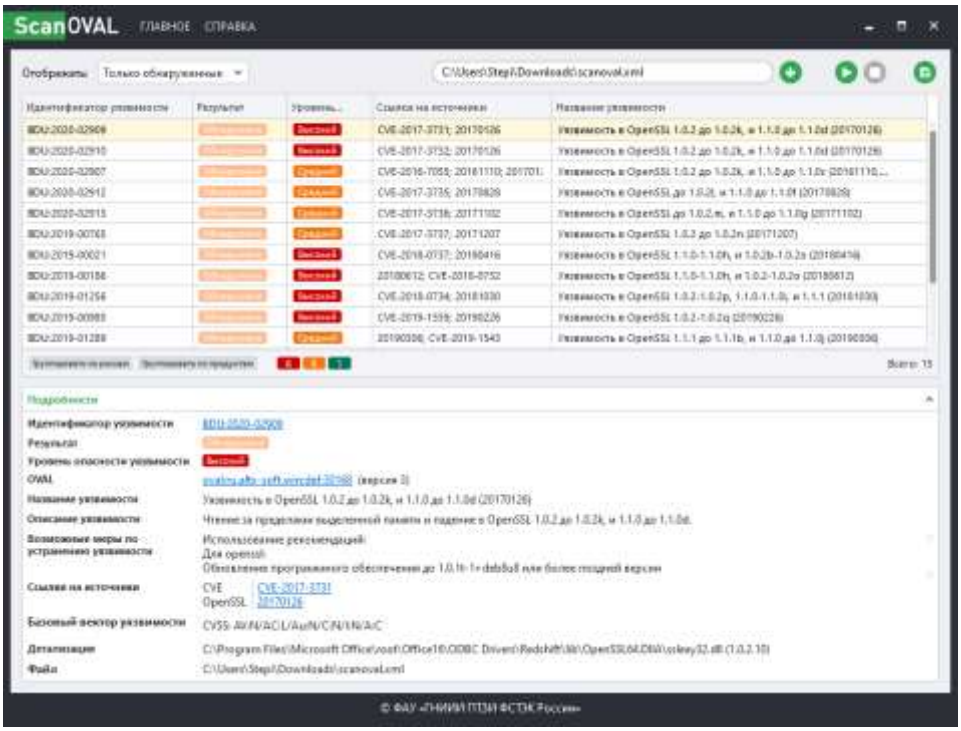

Рисунок 4. Результат попытки устранения уязвимости

Так же при копировании обновленной библиотеки ssleay32.dll по пути C:\Program Files\Microsoft Office\root\Office16\ODBC Drivers\Redshift\lib\OpenSSL64.DIIA\ssleay32.dll удалось устранить 6 уязвимостей с ВЫСОКИМ и 5 уязвимостей со СРЕДНИМ уровнем опасности.

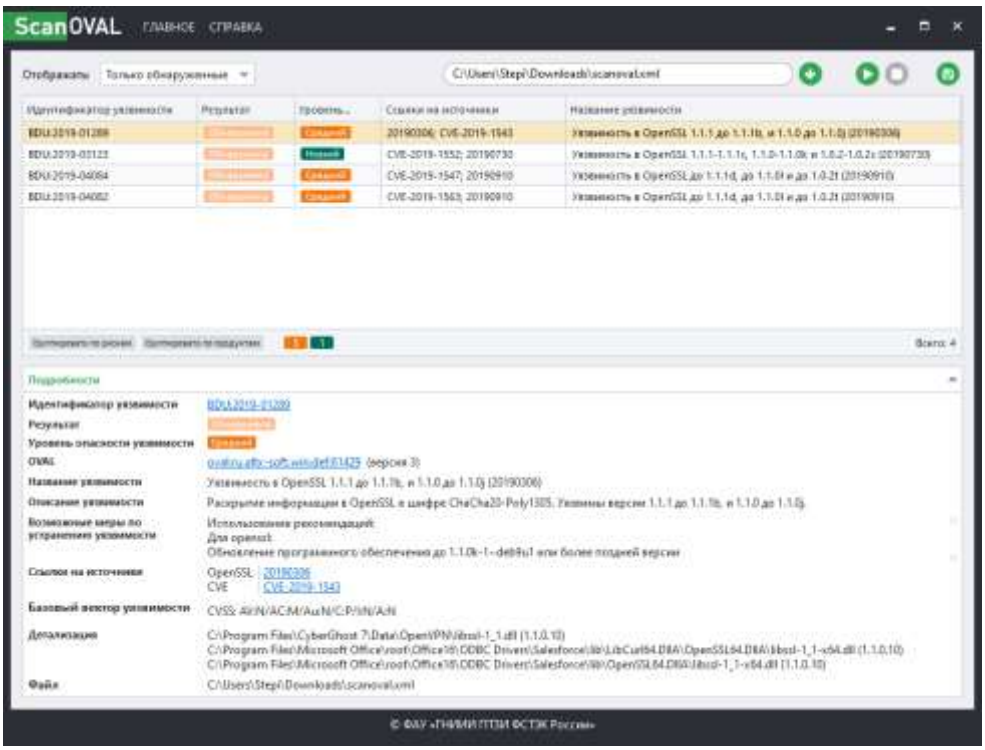

Рисунок 5. Устранение сопутствующих уязвимостей

Выводы

Согласно исследованиям, проводимым различными компаниями («Лаборатория Касперского», Positive Technologies), уязвимости имеются практически в любом приложении, и даже в антивирусах. Поэтому вероятность установки программного продукта, содержащего изъяны разной степени критичности, весьма высока.

В рамках данной статьи, безопасность домашнего ПК была значительно повышена за счет устранения большей части уязвимостей, выявленных программным обеспечением ScanOVAL.

В заключение, хочется отметить, что для минимизации влияния уязвимостей и ущерба от них, необходимо выполнять некоторые правила:

- Оперативно устанавливать выпускаемые разработчиками исправления (патчи) для приложений или (предпочтительно) включить автоматический режим обновления.
- По возможности избегать установки сомнительных программ, чье качество и техническая поддержка вызывают вопросы.

- Использовать специальные сканеры уязвимостей или специализированные функции антивирусных продуктов, позволяющие выполнять поиск ошибок безопасности и при необходимости обновлять ПО.

Использованные источники:

1. Уязвимости программ. [Электронный ресурс]. URL: https://www.anti-malware.ru/threats/programs-vulnerability?page=6 (дата обращения: 10.11.2020).
2. Программа ScanOVAL. [Электронный ресурс]. URL: https://bdu.fstec.ru/site/scanoval (дата обращения: 10.11.2020).
3. Калькулятор CVSS V2. [Электронный ресурс]. URL: https://bdu.fstec.ru/calc (дата обращения: 12.11.2020).