УДК 004.65

РАСЧЕТ ИНФОРМАЦИОННЫХ РИСКОВ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЯ

Э. И. КАМАЛОВА [1], В. М. КАРТАК [2]

[1] kamalova.eliz@yandex.ru, [2] kvmail@mail.ru [2]

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Аннотация. Рассматривается модель архитектуры предприятия и рабочее окружение для разработки веб-приложений. Анализируются уязвимости программного обеспечения среды исполнения согласно “Банку данных угроз безопасности информации” из документа ФСТЭК. Сформированы базовые вектора уязвимостей, по которым определены наибольшие информационные риски при разработке веб-приложений. Представлены мероприятия по устранению уязвимостей в программном обеспечении IT-предприятия.

Ключевые слова: безопасность; информационный риск; веб-приложение; база данных; информационная система (ИС); уязвимость; IT-предприятие; архитектура IT-предприятия.

ВВЕДЕНИЕ

Безопасность веб-приложений находится в первой десятке трендов и угроз информационной безопасности уже свыше 10 лет. Действительно, современные бизнес-процессы и повседневная жизнь – все больше и больше зависит от использования веб-приложений, в разнообразнейших аспектах: от сложных инфраструктурных систем до IT устройств. [1]

Для рассмотрения расчета информационных рисков веб-приложений необходимо ознакомиться с основными терминами и определениями.

Веб-приложение – это приложение, предоставляющее функциональные возможности пользователю через браузер или другой тип агента пользователя, использующего веб-форматы и протоколы. Веб-приложения включают веб-сайты, которые только поставляют информационное наполнение, сочетают доставку контента с характерными для приложения функциональными возможностями или предоставляют только определенные прикладные функциональные возможности, такие как конкретный веб-сервис. [2]

При разработке веб-сайтов возникают уязвимости информационной системы и информационные риски.

Уязвимость – это недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который(-ая) может быть использован(-а) для реализации угроз безопасности информации. [3]

Согласно ГОСТУ 51897-2011 информационный риск – это следствие влияния неопределенности на достижение поставленных целей. А неопределенность – это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей. [4].

Для выявления уязвимостей и их вероятности возникновения необходимо рассмотреть модель архитектуры IT-предприятия и структуру ИС.

МОДЕЛЬ АРХИТЕКТУРЫ IT-ПРЕДПРИЯТИЯ

В архитектуре ИС IT - предприятия, выделяют 4 уровня:

- Уровень инфраструктуры.
- Уровень платформы.
- Замена диска в сервере.
- Переобжим коннектора.
- Подключение нового кабеля.
- Добавление памяти в сервер.

На уровне платформы определяются какие ОС и какие системы виртуализации будут использоваться на “железе”.

На уровне среды исполнения происходит установка, настройка среды исполнения, серверных пакетов и серверных ролей.

На уровне сервисов определяется что нужно конечному потребителю, какой сервис, выбирается программное обеспечение (ПО).

СТРУКТУРА ИС (ВЕБ-ПРИЛОЖЕНИЯ)

Также для расчета и оценки информационных рисков вэб-приложений следует рассмотреть рабочее окружение разработчика. Для работы серверной части (бэкэнда) необходимо установить на персональный компьютер следующее программное обеспечение в зависимости от поставленной операционной системы (рис.1).

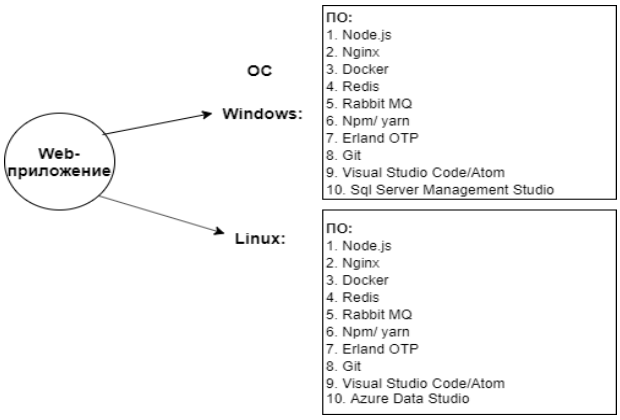

Рис. 1. ПО среды разработки

Согласно “Банку данных угроз безопасности информации” выявлены уязвимости в среде исполнения, к которой относится следующее ПО: Node.js, Nginx, Docker, Redis, Rabbit MQ. [5]

УЯЗВИМОСТИ В ПО.
РАСЧЕТ ИНФОРМАЦИОННЫХ РИСКОВ

Для расчета информационных рисков следует воспользоваться общей системой оценки уязвимостей (Common Vulnerability Scoring System – CVSS). Сформируем для каждой уязвимости базовый вектор и определим уровень опасности.

Самая сильная уязвимость у ПО Node.js - уязвимость парсера URL-адресов Node.js связана с ошибками при обработке HTTP-пакетов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, получить несанкционированный доступ к защищаемым данным с помощью HTTP-запросов. Базовый вектор уязвимости - AV:N/AC:L/Au:N/C:N/I:C/A:N соответствует высокому уровню опасности с численным значением - 7,8.

У веб-сервера Nginx уязвимость реализации протокола HTTP/2 сервера связана с неконтролируемым расходом ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании. Базовый вектор уязвимости - AV:N/AC:L/Au:N/C:N/I:N/A:C соответствует высокому уровню опасности с численным значением -7,8.

Также присутствует уязвимость реализации сетевого протокола HTTP/2 операционных систем Windows, сервера Nginx, сетевых программных средств netty, Envoy, SwiftNIO, программной платформы Node.js связана с неконтролируемым расходом ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании с помощью потока кадров типа DATA, HEADERS, CONTINUATION или PUSH_PROMISE (с пустым полезным содержимым и без флага завершения потока). Базовый вектор уязвимости - AV:N/AC:L/Au:N/C:N/I:N/A:C соответствует высокому уровню опасности с численным значением -7,8.

У ПО для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации – Docker встречается уязвимость компонента daemon/archive.go средства автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации, позволяющая нарушителю повысить свои привилегии и получить доступ на чтение и запись файлов. Базовый вектор уязвимости - AV:L/AC:H/Au:N/C:C/I:C/A:C соответствует среднему уровню опасности с численным значением - 6,2.

У ПО Redis - резидентная система управления базами данных класса NoSQL с открытым исходным кодом, работающая со структурами данных типа «ключ — значение» критический уровень опасности с численным значением – 10 и базовым вектором AV:N/AC:L/Au:N/C:C/I:C/A:C. Уязвимость компонента deps/lua/src/ldo.c системы управления базами данных Redis связана с некорректным преобразованием типа

данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный Lua-байт-код при помощи специально сформированной eval-команды.

У ПО RabbitMQ встретилась уязвимость компонента org.springframework.core. serializer.DefaultDeserializer приложения для обмена сообщениями Spring AMQP RabbitMQ существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код). Базовый вектор уязвимости - AV:N/AC:L/Au:N/C:P/I:P/A:P соответствует высокому уровню опасности с численным значением -7,5. [5].

МЕРОПРИЯТИЯ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ В ПО

Таблица 1

Уязвимость	Класс уязвимости	Возможные мероприятия по устранению
BDU:2019-02939 ПО Node.js	архитектуры	https://nodejs.org/en/blog/vulnerability/november-2018-security-relea https://github.com/nodejs/node/commit/513e9747a22386bc9c93a12f5 1827a1e631
BDU:2019-00982 ПО Nginx	кода	Обновить ПО Nginx до версии 1.15.6, 1.14.1 или новее
BDU:2019-02957 ПО Nginx	кода	Обновить ПО Node.js до версий: Node.js 8.16.1: https://nodejs.org/dist/latest-v8.x/ Node.js 10.16.3: https://nodejs.org/dist/latest-v10.x/ Node.js 12.8.1: https://nodejs.org/dist/latest-v12.x/
BDU:2019-02690 ПО Docker	кода	Ограничение использования программного средства
BDU:2015-10357 ПО Redis	кода	Обновление ПО Redis до версий 2.8.21, 3.0.2 или более новых
BDU:2017-01288 ПО RabbitMQ	кода	Пользователи уязвимых версий должны применять следующие м • Указанный класс (DefaultDeserializer) не регистрируется одним контекстом приложения Spring автоматически; пользователи должны соблюдать осторожность при использовании этого класса с объектами из ненадежных источников так же, как при непосредственном использов ObjectInputStream. • Spring AMQP имеет (дополнительный) конвертер сообщ который может использовать этот десериализатор; начин версии 1.5.5, этот конвертер теперь может быть настроен белым списком приемлемых пакетов / классов, которые десериализовать. • Spring AMQP также имеет SimpleMessageConverter, котс настроен * по умолчанию; он не использует десериализа но использует ObjectInputStream внутри; теперь его такж можно настроить с помощью белого списка пакетов / кл • Пользователям не рекомендуется использовать сериализ Java при использовании RabbitMQ в среде, где могут бы получены ненадежные данные; если они это сделают, он должны настроить конвертер с допустимыми объектами • Пользователи, которые могут быть подвержены этой уязвимости, должны выполнить обновление до Spring A 1.5.5 или выше и настроить белый список.

Для ликвидации возникших уязвимостей в ПО среды разработки (табл.1) необходимо своевременно обновлять версии используемых пакетов. В документе ФСТЭК “Банк данных угроз безопасности информации” имеется информация о том, в какой версии встречалась уязвимость и в каком статусе находится на данный момент. [5].

ЗАКЛЮЧЕНИЕ

В данной статье были рассмотрены модель архитектуры IT-предприятия и структура веб-приложения. Выявлены уязвимости в среде исполнения и их уровни опасности с численными значениями. Представлены мероприятия по устранению уязвимостей в программном обеспечении IT-предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646). [Information Security Doctrine of the Russian Federation (approved by Decree of the President of the Russian Federation of December 5, 2016 No. 646).]

2. **ГОСТ Р ИСО 9241-151-2014.** Эргономика взаимодействия человек-система. Часть 151. Руководство по проектированию пользовательских интерфейсов сети Интернет (Переиздание). [Ergonomics of human-system interaction. Part 151. Manual on the design of user interfaces for the Internet (Reprint), Federal standard R ISO 9241-151-2014.]

3. **ГОСТ Р 56546-2015.** Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. [Information protection. Vulnerabilities of information systems. Classification of vulnerabilities in information systems, Federal standard R 56546-2015]

4. **ГОСТ Р 51897-2011.** Менеджмент риска. Термины и определения. [Risk management. Terms and Definitions, Federal standard R 51897-2011.]

5. ФСТЭК России “Банк данных угроз безопасности информации”. [FSTEC Russia “Information Security Threat database”.]

ОБ АВТОРАХ

КАМАЛОВА Элизабет Ильшатовна, магистрант 2-го курса факультета вычислительной техники и защиты информации.

КАРТАК Вадим Михайлович, зав. кафедрой ВТиЗИ, д-р физ.-мат. наук, доцент.

METADATA

Title: Estimation of security information risks of web applications

Authors: E. I. Kamalova [1], V. M. Kartak[1].

Affiliation:

Ufa State Aviation Technical University (UGATU), Russia.

Email: [1] kamalova.eliz@yandex.ru, [2] kvmail@mail.ru,

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), no. 1 (22), pp. 81-84, 2020. ISSN 2225-9309 (Print).

Abstract: In this paper we are reviewing the model of enterprise architecture and the working environment for developing web applications. Vulnerabilities of the runtime environment application are analyzed according to the "Information Security Threat Databased" from the FSTEC document. The basic vulnerability vectors are formed, according to which the greatest information risks are determined during the development of web applications. Vulnerability removal measures for IT enterprise software are presented.

Key words: data security; information risk; web application; database; information system (IS); web application vulnerability; IT enterprise; architecture of an IT enterprise.

About authors:

KAMALOVA, Elizabeth Ilshatovna, 2nd year of Master's program at the Dept. of Computing Engineering and Information Security.

KARTAK, Vadim Mikhailovich, Prof., Dept. of Computing Engineering and Information Security. Dr. of Phys. And Math. Sci, Associate Professor.