УДК 004.492.2

Мошнина А.А.,
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.

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ MS OFFICE

Аннотация: *В данной статье проводится исследование уязвимостей в программном обеспечении Microsoft Office. Автором анализируются такие уязвимости в данном ПО как удаленное выполнение кода, повышение привилегий и отказ в обслуживании. Рассмотрены методы их устранения. Исследование проводилось с помощью программного обеспечения ScanOVAL.*

Ключевые слова *Уязвимость, защита, программное обеспечение, информационные сети, безопасность, ScanOVAL.*

Annotation: *This article examines vulnerabilities in Microsoft Office software. The author analyzes such vulnerabilities in this SOFTWARE as remote code execution, privilege escalation, and denial of service. Methods of their elimination are considered. The study was conducted using the ScanOVAL software.*

Key words: *Vulnerability, security, software, information networks, security, ScanOVAL.*

Сегодня Microsoft Office является самым популярным пакетом ПО в мире. В нем обрабатываются большие объемы данных, и это делает его крайне привлекательным для злоумышленников, которые постоянно совершенствуют инструменты атак и выбирают все более эффективные способы взлома.

Программы, относящиеся к MS Office: Word, Excel, Access, Power Point, Outlook, Photo Draw, Publisher, Internet Explorer.

Уязвимость – это ошибки в программном обеспечении, оборудовании или организационных процессах, которые, будучи скомпрометированы угрозой, могут привести к нарушению безопасности.

Способ использования компьютерной уязвимости зависит от характера уязвимости и мотивов злоумышленника. Эти уязвимости могут возникать из-за непредвиденных взаимодействий различных программ, компонентов системы или основных дефектов в отдельной программе.

5 простых шагов для оценки уязвимости безопасности любой сети:

- определить и реализовать подход компании или отрасли, например, как она структурирована и управляется;
- проследить за данными, системами и приложениями, которые используются на протяжении всего времени;
- классифицировать виртуальные и физические серверы, на которых выполняются основные приложения;
- отслеживать все существующие меры безопасности, которые уже реализованы;
- проверить сеть на наличие любых уязвимостей [1].

Проверить сеть на уязвимости можно с помощью сканера уязвимостей – это то программное обеспечение, которое может обнаруживать уязвимости в сети, системе или приложении.

Сканеры уязвимостей автоматизируют аудит безопасности и могут играть жизненно важную роль в IT-безопасности, сканируя сеть и веб-сайты на наличие различных рисков безопасности. Эти сканеры также способны генерировать приоритетный список, описать уязвимости и предоставить шаги по их устранению. Кроме того, некоторые из них могут даже автоматизировать процесс исправления.

Для поиска уязвимостей в программном обеспечении Microsoft Office был использован сканер уязвимостей ScanOVAL. Запуск программы требует привилегий администратора на локальном ПК. Для поиска в том числе и новых уязвимостей необходимо провести актуализацию базы уязвимостей с сайта БДУ ФСТЭК.

Для того чтобы программа сканирования работала, аппаратная конфигурация компьютера должна соответствовать следующим минимальным требованиям:

- 32-битный (x86) или 64-битный (x64) процессор с тактовой частотой 1 ГГц и выше;

- 1 ГБ (для 32-битной системы) или 2 ГБ (для 64-битной системы) оперативной памяти;

- 0,5 ГБ свободного места на жестком диске.

Наиболее часто встречаемые уязвимости Microsoft Office: удаленное выполнение кода, повреждение памяти, отказ в облуживании, уязвимость повышенных привилегий.

Перейдем к более подробному рассмотрению некоторых из них.

1. Уязвимость удаленного выполнения кода Microsoft Office. С помощью сайта БДУ ФСТЭК видим идентификатор типа ошибки, уровень безопасности уязвимости, статус производительности (рисунок 1).

Рисунок 1. Характеристики уязвимости

На рисунке 2 представлена уязвимость оценки с помощью калькулятора CVSS.

Рисунок 2. Оценка уязвимости

Многочисленные уязвимости удаленного выполнения кода существуют в программном обеспечении Microsoft Office, когда программное обеспечение Office не может должным образом обрабатывать объекты в памяти. Злоумышленник, успешно воспользовавшийся уязвимостями, может запустить произвольный код в контексте текущего пользователя. Если текущий пользователь вошел в систему с правами администратора, злоумышленник может получить контроль над уязвимой системой. Затем злоумышленник может устанавливать программы, просматривать, изменять или удалять данные, а также создавать новые учетные записи с полными правами пользователя. Пользователи, учетные записи которых настроены так, чтобы иметь меньше прав пользователя в системе, могут подвергаться меньшему воздействию, чем пользователи, работающие с правами администратора [2].

Использование уязвимостей требует, чтобы пользователь открыл специально созданный файл с уязвимой версией программного обеспечения Microsoft Office. В случае атаки по электронной почте злоумышленник может воспользоваться уязвимостями, отправив пользователю специально созданный файл и убедив его открыть его. В сценарии веб-атаки злоумышленник может разместить веб-сайт (или использовать скомпрометированный веб-сайт, который принимает или размещает предоставленный пользователем контент), содержащий специально созданный файл, предназначенный для использования уязвимостей. Злоумышленник должен убедить пользователей перейти по ссылке, как правило, путем привлечения в сообщении электронной почты или мессенджера, а затем убедить их открыть специально созданный файл [3].

Решение проблемы удаленного выполнения кода (3104540) – это обновление безопасности Microsoft Office. Данное обновление для системы безопасности устраняет уязвимости путем:

- исправления того, как Office обрабатывает объекты в памяти;
- обеспечения того, что Microsoft Excel предотвращает создание;

экземпляров уязвимых приложений Office.

2. Вместе с уязвимостью удаленного доступа часто присутствует уязвимость повышения привилегий (рисунок 3).

Рисунок 3. Уязвимость повышенных привилегий

Она существует в программном обеспечении Microsoft Office, когда злоумышленник создает экземпляр открытого приложения Office. Злоумышленник, успешно воспользовавшийся уязвимостью, может получить повышенные привилегии и выйти из изолированной среды Microsoft Excel. Чтобы успешно использовать эту уязвимость, злоумышленник должен воспользоваться существующей уязвимостью в Microsoft Excel, обманув пользователя и загрузив специально созданное приложение. Скорее всего, эта уязвимость будет использоваться в сочетании с другой уязвимостью, которая допускает удаленное выполнение кода. Например, злоумышленник может использовать другую уязвимость для запуска произвольного кода через Microsoft Excel, но из-за контекста, в котором процессы запускаются Microsoft Excel, код может быть ограничен для запуска на низком уровне целостности (очень ограниченные разрешения). Однако злоумышленник может, в свою очередь, воспользоваться этой уязвимостью, чтобы заставить произвольный код выполняться на среднем уровне целостности (разрешения текущего пользователя). Обновление для системы безопасности устраняет эту уязвимость, гарантируя, что Microsoft Excel предотвращает создание экземпляров затронутых офисных приложений. Эта уязвимость была

публично раскрыта. Ему был присвоен общий номер уязвимости и подверженности этой уязвимости [CVE-2015-2503] [4].

Уязвимость подмены существует, когда Microsoft не дезинфицирует HTML или не обрабатывает его безопасным способом. Злоумышленник, успешно воспользовавшийся этой уязвимостью, может обмануть пользователя, перенаправив его на вредоносный веб-сайт. Вредоносный веб-сайт может подделывать контент или использоваться в качестве стержня для цепочки атак с другими уязвимостями в веб-службах. Чтобы воспользоваться этой уязвимостью, пользователь должен предварительно просмотреть злонамеренно созданное электронное письмо от злоумышленника, где он будет неосознанно перенаправлен на вредоносный URL-адрес.

Обновление устраняет эту уязвимость, исправляя то, как Microsoft Office проверяет и дезинфицирует HTML-ввод.

3. Следующая уязвимость – уязвимость, приводящая к отказу в обслуживании Microsoft Office. Уязвимости, приводящие к отказу в обслуживании, в основном вызваны ошибками в проверках входных данных, некорректной работой с памятью (ошибки при работе с переменными в стеке, неверная работа с указателями), бесконтрольным выделением ресурсов. Эксплуатация подобных уязвимостей приводит к недоступности сервисов на сетевом периметре.

У большинства клиентов включено автоматическое обновление, и им не нужно будет предпринимать никаких действий для устранения уязвимости, поскольку это обновление для системы безопасности будет загружено и установлено автоматически. Клиенты, которые не включили автоматическое обновление, должны проверить наличие обновлений и установить его вручную.

Далее рассмотрим способы, которые заставляют Microsoft Office выполнять код, встроенный в документ. Ниже приведены 2 из наиболее популярных методов для выполнения кода.

1. Макросы VBA

Поддержка выполнения кода, встроенного в виде макроса VBA (Visual Basic for Applications), встроена в Microsoft Office. Как только жертва открывает документ и разрешает запуск макросов, этот код может запускать произвольные команды в системе пользователя, включая те, которые запускают программы и взаимодействуют по сети.

Такие макросы могут быть включены в устаревшие двоичные форматы (.doc, .xls., .ppt) и в современные XML-форматированные документы, поддерживаемые Microsoft Office 2007 и выше. В любом случае Office выдаст пользователю предупреждение о безопасности, сообщив, что макросы отключены, и предложит "включить контент" (рисунок 4). Методы социальной инженерии могут убедить жертву нажать кнопку, которая позволит встроенному макросу запустить и заразить систему.

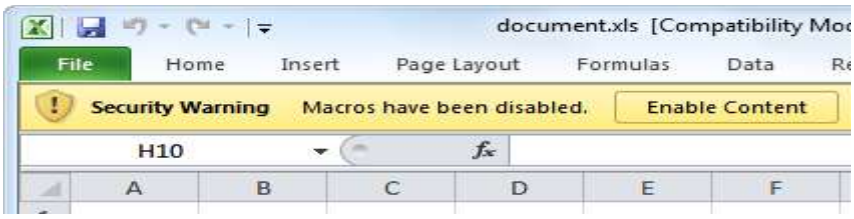

Рисунок 4. Пример уведомления предупреждения

2. Полезная нагрузка эксплойта Microsoft Office

Другой способ выполнения вредоносного кода как части документа Office включает использование уязвимостей в приложении Microsoft Office. Эксплойт предназначен для того, чтобы обманом заставить целевое приложение выполнить полезную нагрузку злоумышленника, которая обычно скрывается в документе Office в виде шелл-кода.

Например, уязвимость выполнения удаленного кода может позволить злоумышленнику создать вредоносный файл Excel для включения эксплойта, который возьмет полный контроль над уязвимой системой.

Это некоторые из методов, которые злоумышленники используют для выполнения кода в документах Microsoft Office, чтобы скомпрометировать систему. Злоумышленник может напрямую воспользоваться уязвимостью в

целевом приложении Office. В других случаях злоумышленник использует функциональные возможности, предоставляемые Microsoft Office, чтобы либо обмануть пользователя, позволяя вредоносному коду работать (макросы VBA), либо использовать слабость в настройках Office для запуска кода, который использует уязвимости в других приложениях.

В данной статье были рассмотрены уязвимости Microsoft Office. Для их устранения рекомендуется установить автоматическое обновления программ или же переустановить Office на более новую версию. Корпоративные правила обновления могут задерживать своевременное обновление и, возможно, часть пользователей не может отказаться от устаревших неподдерживаемых версий, что приводит к необходимости выработки правил работы с документами и проверки их происхождения.

Использованные источники:

1. Пиховкин, Н.Л. Обеспечение безопасности распределенной информационно-вычислительной сети с учетом управления рисками / Пиховкин Н.Л., Сахаров Д.В. // Труды учебных заведений связи. 2016. Т. 2. № 2. С. 93-97.
2. Топ-10 сканеров оценки уязвимости [Электронный ресурс]. URL: https://cwatch.comodo.com/blog/website-security/top-10-vulnerability-assessment-scanning-tools/ (дата обращения 10.11.2020).
3. Красов, А.В. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения / Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36-40.
4. Национальная база данных по уязвимостям. Электронный ресурс. URL: https://nvd.nist.gov/vuln/detail/CVE-2020-16957 (дата обращения 11.11.2020).