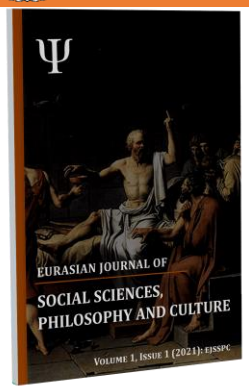
EURASIAN JOURNAL OF SOCIAL SCIENCES, PHILOSOPHY AND CULTURE
Innovative Academy Research Support Center
UIF = 8.2 | SJIF = 6.051 www.in-academy.uz



УЯЗВИМОСТИ НУЛЕВОГО ДНЯ И РЕКОМЕНДАЦИИ ПО УМЕНЬШЕНИЮ РИСКА ЭКСПЛУАТАЦИИ

Айсаев Искандар Музаффарович
aysaev.ir@gmail.com
ведущий специалист ГУП «Центр кибербезопасности»
https://doi.org/10.5281/zenodo.7149124

ARTICLE INFO

Received:30th September 2022
Accepted: 03rd October 2022
Online: 05th October 2022

KEY WORDS

информационная безопасность, кибербезопасность, атаки, взлом систем, нулевой день, мессенджеры, хакеры-злоумышленники.

ABSTRACT

Данная статья посвящена актуальной проблеме нулевого дня в обеспечении информационной и кибербезопасности, где рассмотрены возможные угрозы кибербезопасности, раскрыто понятие нулевого дня. А также, даны пояснения к защите от атак нулевого дня, описаны методы обеспечения информационной и кибербезопасности.

Введение

Часто в новостных лентах мы читаем о новых и опасных, так называемых, уязвимостях нулевого дня или “zero day”. Но что это за уязвимости?

Из самого наименования можно понять, что у программистов не было ни одного дня, то есть, не было никакой возможности устранить проблему в коде, так как они про них просто не знали. Об уязвимости становится известно до того момента, когда производитель программного обеспечения выпустит обновление с исправлением, или новую версию программы. Таким образом, до этого момента, все устройства, работающие с этим ПО подвергаются риску.

В любой программе есть свои недочёты. Информационные системы массового использования приносят наибольший ущерб для пользователей. Уязвимости нулевого дня занимают высокий уровень серьезности и активно применяются хакерами. Атаку нулевого дня можно считать одной из самых опасных, потому что невозможно огородиться от того, чего не знаешь. Одной из известных атак нулевого дня можно считать серию атак на Google Chrome в 2021 году ставших причиной ряда обновлений Chrome. Уязвимость активировалась из-за некорректной работы в JavaScript-коде V8, используемом в веб-браузере.

Основная часть

2021 год прошел под большим количеством кибер-атак, поиска аппаратных уязвимостей и громких утечек. За то время, пока руководители компаний приходили к осознанию необходимости выстраивать действительно эффективную систему информационной и кибербезопасности,

злоумышленники прочно обосновались в киберпространстве. в частности, связано с созданием новых эффективных программных средств деструктивных информационных воздействий. Это связано с тем, что западные страны стали создавать и финансировать кибервойска. Кроме того, преступники продолжают использовать неграмотность пользователей в вопросах обеспечения информационной и кибербезопасности.

Злоумышленники активно используют новейшие уязвимости, действуют очень быстро, а главное — часто меняют инструментарий и тактики. Непосредственная угроза сложных целенаправленных атак побуждает компании по-новому взглянуть на эффективность систем защиты.

Сегодня киберпреступники — это настоящие профессионалы, у которых есть финансовая мотивация, часто работающие под эгидой организованных преступных групп, радикальных политических партий и даже злонамеренных государств. Это высококвалифицированные специалисты, в распоряжении которых появились отличные ресурсы. Брандмауэры, антивирусное ПО и меры по фильтрации контента не могут их сдержать.

Взлом системы безопасности может привести к потере или краже критичной для компании информации, что вызовет тяжелые экономические последствия. Такой взлом также может разрушить репутацию компании. Даже угроза подобной атаки наносит большой ущерб. Руководители подвергаются дополнительному стрессу, который никому не нужен.

Кроме этого, многие кибератаки происходят из-за небрежности. Когда сотрудники открывают вложенные файлы или фишинговые письма, а также совершают другие вроде бы невинные ошибки, это становится причиной около 88% инцидентов, связанных с утечкой данных.

Помимо небрежности особую роль играют уязвимости нулевого дня или zero-day – это ранее неизвестная уязвимость, которая эксплуатируется злоумышленниками в сетевых атаках. Подобные уязвимости оцениваются как критические.

Происхождение термина связано с тем обстоятельством, что уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от нее).

Злоумышленник замечает уязвимость ПО еще до того, как производить ее обнаружил, быстро создает эксплойт и использует его для проникновения. Такие атаки с большой вероятностью увенчаются успехом. Это делает уязвимости нулевого дня серьезной угрозой безопасности. При атаках нулевого дня могут использоваться различные уязвимые объекты: Операционные системы, Веб-браузеры, Офисные приложения, Компоненты с открытым исходным кодом; Аппаратное обеспечение и Интернет вещей.

Наибольший риск для пользователей создают именно продукты массового

использования, такие как популярный Adobe Reader.

В результате атак нулевого дня список жертв становится достаточно широким:

1. Лица, использующие уязвимые системы, такие как браузер или операционная система. Хакеры могут использовать уязвимости системы безопасности для взлома устройств и создания крупных ботнетов.
2. Лица, имеющие доступ к ценным бизнес-данным, таким как интеллектуальная собственность.
3. Крупные предприятия и организации.
4. Государственные организации.
5. Политические объекты и объекты национальной безопасности.

Особую опасность такие уязвимости представляют потому, что максимально увеличивают шансы на успех кибератаки. Главный и самый позитивный вывод отчета по выявленным уязвимостям: 2021 год стал рекордным по обнаружению zero-day, всего уязвимостей нулевого дня было обнаружено 58, более чем в два раза больше, чем в 2020 году.

Логика «чем больше уязвимостей, тем лучше» может показаться сомнительной, но на самом деле лучше, когда активно эксплуатируемые уязвимости обнаруживают, чем когда они остаются неизвестными долгое время.

Для zero-day будет правильнее говорить о корректной классификации: разработчики, по мнению специалистов в области кибербезопасности, должны более активно делиться информацией о zero-day. В качестве положительных примеров добровольного раскрытия информации приводятся компания Apple и команда разработки ОС Android в самой Google. Соответственно с ноября 2020 года и с января 2021 года при раскрытии информации об уязвимости они начали помечать активно эксплуатируемые. Раскрывать информацию о том, что прореха в софте кем-то эксплуатировалась до обнаружения, могут и независимые исследователи.

Но они не всегда являются источником информации о zero-day. Так, информация о 12 уязвимостях из 58 в прошлом году была прислана вендору анонимно: то есть обнаруживший ее не планировал независимо раскрывать информацию.

Специалисты в области кибербезопасности отмечают рост количества источников информации о zero-day, то есть больше организаций или частных лиц так или иначе заняты обнаружением и доведением до общественности информации об эксплуатируемых уязвимостях. Тем не менее специалисты допускают, что знаем мы далеко не обо всех прорехах нулевого дня. В пример приводятся мессенджеры типа Whatsapp, Telegram, iMessage, доступ к переписке которых — ценный приз для организаторов кибератак. Тем не менее в базе Project Zero с 2014 года зафиксировано только две уязвимости — одна для Whatsapp в 2019 году, другая для iMessage в 2021 году. Напомним, речь идет об уязвимостях нулевого дня — тех, о которых вендор узнает уже тогда, когда проблема эксплуатируется. Можно предположить, что zero-day в мессенджерах больше, просто либо мы о них вообще не знаем, либо

разработчики закрывают их, не объявляя о факте эксплуатации.

Специалисты по кибербезопасности напрямую занимающиеся поиском и эксплуатации уязвимостей ставят перед собой цель по отслеживанию zero-day уязвимостей.

Специалисты отмечают, что выявленные 39 уязвимостей из 58, то есть две трети, относятся к типу «повреждение содержимого в оперативной памяти». В целом только две уязвимости 2021 года были отмечены как инновационные. Это означает, что одно только применение мер по снижению количества уязвимостей типа memory corruption или по затруднению их эксплуатации серьезно усложнит жизнь атакующим. Пока же речь скорее идет о том, что существующие инструменты атаки легко перенацелить на другую уязвимость, если предыдущая закрывается вендором, — так как тип уязвимости и метод взлома могут быть похожими.

Специалисты по кибербезопасности признают наличие множества белых пятен в процессе изучения zero-day, причин их применения и методов эксплуатации. Нам может быть не известно о каких-то реально инновационных методах атаки на ПО и сервисы. Хотя практика показывает, что организаторы атак тоже стараются экономить ресурсы.

Иногда бывают случаи, когда ошибку могут найти пользователи или сами разработчики, после чего производителями выпускается новая версия ПО или обновление. Кроме того, антивирусы тоже иногда могут зарегистрировать вредоносные действия.

Впрочем, очевидно, что обнаружить баг могут и хакеры-злоумышленники, преследующие вредоносные цели. Тогда они будут эксплуатировать его сами или продадут другим киберпреступникам. Для обнаружения уязвимостей злоумышленники используют различные методы:

1. дизассемблирование кода программы и поиск опасных ошибок в коде программного обеспечения;
2. fuzz-тестирование или «стресс-тест» для ПО (программное обеспечение обрабатывает большой объем информации, которая содержит заведомо ложные настройки);
3. реверс-инжиниринг и поиск уязвимостей в алгоритмах работы ПО.

В противоположном случае разработчик знает, что существует баг в коде, но не хочет или не может его устранить, не предупреждая никого об уязвимости. Если произошла атака с использованием уязвимости нулевого дня, то это значит, что злоумышленники знали о баге достаточное количество времени, чтобы написать и активировать вредоносную программу для его эксплуатации. Такие атаки опасны тем, что к ним невозможно подготовиться, а также тем, что постоянное обновление ПО не дает гарантии их предотвращения или снижения риска их возникновения.

Еще одно важное «белое пятно» — это особенности самих эксплойтов, точнее отсутствие информации о них. Иногда ее просто нет, иногда данные не раскрываются. Только для пяти из 58 уязвимостей был публично доступен эксплойт. Доступность эксплойтов для

исследователей позволяет изучать не только сами уязвимости, но и методы атаки, и там тоже усложнять жизнь организаторам этих атак. И это, пожалуй, самый скользкий и интересный момент. С одной стороны, обмен информацией в индустрии информационной безопасности повышает защиту. С другой — публичные эксплойты часто приводят к массовым атакам на ПО, пропатчить которое вовремя удается не всегда.

Защита от уязвимостей нулевого дня и их устранение ошибок входит в обязанности разработчика. Критическая проблема закрывается в течение нескольких дней или недель; все это время системы, использующие уязвимое ПО, будут находиться в опасности.

Для защиты от атак нулевого дня и обеспечения безопасности компьютеров и данных частным лицам и организациям важно выполнять определенные правила кибербезопасности. Они включают:

1. Своевременное обновление программ и операционных систем. Производители включают в новые выпуски исправления безопасности для устранения недавно обнаруженных уязвимостей. Своевременное обновление повышает вашу безопасность.
2. Использование только необходимых программ. Чем больше у вас программного обеспечения, тем больше потенциальных уязвимостей. Использование только необходимых программ позволит снизить риск для сети.
3. Использование межсетевого экрана. Межсетевой экран играет важную роль в защите системы от угроз нулевого дня. Настройка межсетевого экрана так, чтобы допускались только необходимые транзакции, позволит обеспечить максимальную защиту.
4. Обучение сотрудников организаций. Многие атаки нулевого дня основаны на человеческих ошибках. Обучение сотрудников и пользователей правильным навыкам обеспечения безопасности и защиты поможет как обеспечить их безопасность в интернете, так и защитить организацию от эксплойтов нулевого дня и других цифровых угроз.

Вывод

Почти любая современная компания так или иначе связана с информационными технологиями, определенные её процессы работают с использованием программных продуктов и телекоммуникационных сетей.

Новые уязвимости, вирусы, атаки появляются каждый день. Для защиты от них регулярно выпускаются обновления программного обеспечения и баз данных, своевременная установка которых необходима и обязательна. Масштаб и схема работы системы должны постоянно изменяться в соответствии с изменениями объёмов информации и требований к её защите.

На мой взгляд, время, когда организации, не связанные с IT-сферой, могли игнорировать вопросы защиты информации, подходит к концу. Необходимо оценивать важность информационных ресурсов для функционирования процессов и адекватно защищать их.

Не существует полностью надежных систем, кибербезопасность — это

постоянная борьба. Киберпреступники неустанно ищут любые уязвимости, через которые можно ударить.

Киберугрозы никуда не исчезнут, но их можно избежать или нивелировать последствия, если обладать нужными знаниями и действовать превентивно.

References:

1. Zero-day (computer) https://searchsecurity.techtarget.com/definition/zero-day-vulnerability.
2. Уязвимость нулевого дня (https://www.anti-malware.ru/threats/zero-day);
3. «Нулевой день. Определение и описание» https://www.kaspersky.ru/resource-center/definitions/zero-day-exploit.
4. «Что такое атака нулевого дня? Определение и описание» https://www.kaspersky.ru/resource-center/definitions/zero-day-exploit.
5. «Устранение уязвимостей нулевого дня», 15.09.2022 г. https://learn.microsoft.com/ru-ru/microsoft-365/security/defender-vulnerability-management/tvm-zero-day-vulnerabilities?view=o365-worldwide.
6. Ким Зеттер «Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon», 2014.
7. Диогенес Ю., Озкайя Э. «Кибербезопасность: стратегии атак и обороны», Практическое пособие 2020 г.
8. Хлестова Д.Р., Редников Д.В. «Уязвимости нулевого дня- опасная угроза информационной безопасности», 2017 г.
9. Advanced Persistent Threat (APT) Таргетированные или целевые кибератаки «Развитая устойчивая угроза», 2022 г.
10. Georgia Weidman «Общеметодологическое описание тестов на проникновение и обнаружение уязвимостей».