Авдалян А.А. Внедрение вредоноса в видеодрайверы: можно ли атаковать через OPENGL и VULKAN // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 78–81

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

ВНЕДРЕНИЕ ВРЕДОНОСА В ВИДЕОДРАЙВЕРЫ: МОЖНО ЛИ АТАКОВАТЬ ЧЕРЕЗ OPENGL И VULKAN

Авдалян А.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: sharmanka228@gmail.com

Системы, использующие OpenGL и Vulkan для графических вычислений, становятся всё более сложными и функциональными, что открывает новые возможности для атак. В статье рассматривается возможность внедрения вредоносного кода в видеодрайверы через эти графические API, их уязвимости, методы эксплуатации и способы защиты от подобных атак. Особое внимание уделено архитектурным особенностям драйверов и механизму взаимодействия с операционными системами и приложениями, что делает возможным применение таких атак в реальных сценариях.

Ключевые слова: Вирус, видеодрайверы, OpenGL, Vulkan, атаки, уязвимости, безопасность, графика.

MALWARE INJECTION INTO VIDEO DRIVERS: IS IT POSSIBLE TO ATTACK THROUGH OPENGL AND VULKAN

Avdalyan A.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

Systems using OpenGL and Vulkan for graphics computations are becoming increasingly complex and functional, opening up new avenues for attacks. This article explores the potential for injecting malicious code into graphics drivers through these graphics APIs, their vulnerabilities, methods of exploitation, and ways to protect against such attacks. Special attention is given to the architectural features of drivers and the interaction mechanisms with operating systems and applications, making such attacks viable in real-world scenarios.

Keywords: Malware, graphics drivers, OpenGL, Vulkan, attacks, vulnerabilities, security, graphics.

Введение

С каждым годом графические API, такие как OpenGL и Vulkan, становятся неотъемлемой частью как игр, так и сложных вычислительных задач, включая машинное обучение и научные вычисления. Развитие технологий в этой области привело к значительному увеличению сложности и функциональности видеодрайверов, которые теперь выполняют гораздо больше задач, чем просто рендеринг графики. Однако, с увеличением их функционала растет и количество потенциальных уязвимостей, которые могут быть использованы злоумышленниками для атак. В этом контексте вопросы безопасности видеодрайверов, а также возможность внедрения вредоносного кода через графические API, становятся особенно актуальными.

Внедрение вредоносного кода в видеодрайверы может быть опасным, поскольку эти драйверы имеют высокий уровень привилегий и глубокую интеграцию с операционной системой. Атаки, использующие уязвимости в драйверах, могут привести к удаленному выполнению кода, повышению привилегий или даже к полному контролю над системой. В случае с OpenGL и Vulkan, их широкое распространение и использование в самых различных приложениях создают большие возможности для злоумышленников, желающих использовать графические подсистемы как вектор атак. Этот процесс может быть особенно сложным и малоизученным, поскольку взаимодействие между драйверами, операционной системой и приложениями является многослойным и трудным для мониторинга.

Несмотря на то, что графические драйверы в последние годы значительно улучшились с точки зрения безопасности, они по-прежнему остаются уязвимыми для атак. Злоумышленники могут использовать различные методы эксплуатации уязвимостей, таких как буферные переполнения, некорректное управление памятью и недостаточную изоляцию данных между процессами. Это открывает путь к атакам, где видеодрайверы становятся точкой входа для внедрения вредоносного кода.

Внедрение вредоносного кода через OpenGL и Vulkan

Для начала важно понять, как видеодрайверы работают с OpenGL и Vulkan и какую роль они играют в архитектуре системы. Видеодрайверы — это программы, которые обрабатывают запросы от приложений и операционной системы для отображения графики на экране. OpenGL и Vulkan, являясь стандартами графического рендеринга, позволяют программам запрашивать ресурсы для работы с графическими изображениями, текстурами, шейдерами и т. д. Оба API предоставляют низкоуровневый доступ к видеокарте, что делает их мощными инструментами, но и уязвимыми для атак[1].

OpenGL, будучи более старым API, поддерживает множество устаревших функций и предоставляет широкие возможности для работы с графическими данными, что может открывать дверцу для различных уязвимостей. Vulkan, в свою очередь, обеспечивает более прямой доступ к графическому процессору, что даёт приложениям больший контроль, но также увеличивает риски безопасности. Оба этих API имеют сложную архитектуру взаимодействия между приложениями, драйверами и операционной системой, что может затруднять мониторинг и защиту от атак[2].

Одним из возможных путей атаки через видеодрайверы является внедрение вредоносного кода через недочеты в механизмах обработки данных, передаваемых от приложения в драйвер. Злоумышленники могут использовать уязвимости в обработке шейдеров, текстур или других графических объектов для того, чтобы подменить данные, которые драйвер обрабатывает. Это позволяет внедрять произвольный код в память видеокарты или напрямую в пространство памяти операционной системы, что может привести к выполнению вредоносных команд с высокими привилегиями[3].

Также стоит отметить, что видеодрайверы имеют доступ ко многим системным ресурсам, включая память, устройства ввода-вывода и другие критически важные компоненты. При успешной эксплуатации уязвимости в драйвере, злоумышленник может использовать эту точку доступа для дальнейших атак, таких как повышение привилегий или выполнение команд, которые нарушают целостность системы. Один из таких методов заключается в эксплуатации буферных переполнений, когда приложение или драйвер

пытается записать больше данных в буфер, чем он может вместить. Это приводит к перезаписи памяти и может быть использовано для внедрения вредоносного кода[4].

Кроме того, можно вспомнить о так называемых уязвимостях zero-day, которые в первую очередь ориентированы на драйверы. Это такие уязвимости, которые еще не были раскрыты или исправлены производителями, и их использование может быть крайне опасным для безопасности системы. Изначально эти уязвимости могут быть использованы для проведения атак через OpenGL или Vulkan, особенно когда производители драйверов не уделяют должного внимания проверке и исправлению уязвимостей в своих программных продуктах[5].

Для защиты от подобных атак важно придерживаться нескольких рекомендаций. Во-первых, необходимо регулярно обновлять драйверы и видеодрайверы, поскольку производители часто выпускают обновления, устраняющие уязвимости. Во-вторых, следует использовать средства защиты, такие как изоляция процессов и использование системы контроля целостности, которая поможет обнаружить изменения в видеодрайверах или других критически важных компонентах системы. Также важно использовать системы обнаружения вторжений, которые могут мониторить аномалии в поведении графических драйверов и своевременно предупреждать о возможных угрозах.

Заключение

Внедрение вредоносного кода через видеодрайверы, использующие OpenGL и Vulkan, представляет собой реальную угрозу для информационной безопасности. Уязвимости в этих драйверах могут быть использованы для выполнения кода с повышенными привилегиями, что открывает путь для более серьёзных атак, включая шифрование данных, повышение привилегий и удалённое управление системой. При этом сложность архитектуры драйверов и их тесная интеграция с операционной системой создают дополнительные трудности в защите от таких атак.

Понимание того, как работают графические API и их взаимодействие с операционной системой, а также принятие мер по защите, таких как обновление драйверов и использование систем мониторинга, помогает уменьшить риски. Внедрение вредоносного кода через OpenGL и Vulkan может стать эффективным вектором атак, если системы безопасности не будут своевременно обновляться и адаптироваться к новым угрозам.

Список литературы

1. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Чмутов М. В. и др. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре //Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. – 2017. – С. 535-537.

4. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.
5. Казанцев А. А., Прохоров М. В., Худякова П. С. Обзор подходов к классификации текстов актуальными методами //Экономика и качество систем связи. – 2021. – №. 1 (19). – С. 57-67.

References

1. Krasov A.V., Sakharov D. V., Tasyuk A. A. Designing an intrusion detection system for an information network using big data //High–tech technologies in Earth space research. 2020. – Vol. 12. – No. 1. – pp. 70-76.
2. Minyaev A. A. A method for evaluating the effectiveness of an information security system geographically distributed personal data information systems //Actual problems of infotelec communications in science and education (APINO 2020), 2020, pp. 716-719.
3. Chmutov M. V. and others. A study of the current IT infrastructure of an organization for the subsequent transition to a cloud architecture //Information security of the regions of Russia (IBRD-2017). Conference materials. 2017. pp. 535-537.
4. Petrova T. V. et al. Approaches to detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.
5. Kazantsev A. A., Prokhorov M. V., Khudyakova P. S. Review of approaches to text classification by current methods //Economics and quality of communication systems. – 2021. – №. 1 (19). – pp. 57-67.