Троян И.В. Минимизация временных файлов для предотвращения утечек данных из базы // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 1(51) с. 181–184

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.736

МИНИМИЗАЦИЯ ВРЕМЕННЫХ ФАЙЛОВ ДЛЯ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ ИЗ БАЗЫ

Троян И.В.
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: it.bonch@gmail.com

Временные файлы, создаваемые системами управления базами данных (СУБД), являются важной частью работы с запросами, но при неправильной настройке они могут стать источником утечки данных. В статье рассматриваются риски, связанные с временными файлами, такие как несанкционированный доступ и эксплуатация остаточных данных, а также предлагаются методы минимизации их использования, включая шифрование, ограничение прав доступа и оптимизацию запросов.

Ключевые слова: Временные файлы, утечка данных, базы данных, безопасность СУБД, шифрование, оптимизация запросов, минимизация рисков.

MINIMIZING TEMPORARY FILES TO PREVENT DATA LEAKS FROM DATABASES

Troyan I.V.
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: it.bonch@gmail.com

Temporary files created by database management systems (DBMS) are an essential part of query processing, but when improperly managed, they can become a source of data leaks. This article explores the risks associated with temporary files, such as unauthorized access and residual data exploitation, and suggests methods to minimize their usage, including encryption, access control, and query optimization.

Keywords: Temporary files, data leaks, databases, DBMS security, encryption, query optimization, risk minimization.

Введение

Современные системы управления базами данных (СУБД) обрабатывают огромные объёмы данных, и временные файлы являются неотъемлемой частью этого процесса. Они используются для хранения промежуточных результатов выполнения сложных запросов, операций сортировки и индексации. Однако, несмотря на их важность, временные файлы могут стать уязвимым местом в системе безопасности базы данных. Остаточные данные, сохраняемые во временных файлах, часто остаются без должного внимания и защиты, что делает их привлекательной целью для злоумышленников.

Утечка данных из временных файлов может произойти через несанкционированный доступ к системам хранения, уязвимости операционной системы или даже через ошибки в конфигурации самой СУБД. Это особенно критично для организаций, работающих с конфиденциальной информацией, включая финансовые данные, персональные данные

пользователей или коммерческую тайну. Задача минимизации временных файлов заключается не только в их ограничении, но и в создании многоуровневой защиты, предотвращающей потенциальные утечки.

Минимизация временных файлов для предотвращения утечек данных из базы

Использование временных файлов в СУБД связано с необходимостью обеспечения высокой производительности при выполнении ресурсоёмких операций. Например, временные таблицы могут использоваться для хранения промежуточных данных при выполнении сложных SQL-запросов с объединением таблиц или при обработке больших объёмов данных. Однако каждая такая операция увеличивает риск утечки данных, если временные файлы не защищены должным образом[1].

Одной из основных проблем является сохранение остаточных данных во временных файлах. Даже после завершения запроса или удаления временного файла информация может оставаться в системе хранения в виде фрагментов, которые могут быть восстановлены злоумышленниками с помощью специальных инструментов. Это особенно опасно в условиях, когда диски, на которых хранятся временные файлы, недостаточно защищены или не используют механизмы шифрования[2].

Важным шагом к минимизации утечек данных через временные файлы является шифрование. Многие современные СУБД, такие как PostgreSQL, MySQL и Microsoft SQL Server, поддерживают шифрование временных файлов. Эта функция позволяет зашифровать данные на уровне хранения, делая их недоступными для несанкционированного доступа даже в случае компрометации системы. Однако шифрование не решает всех проблем — требуется также контроль за доступом к файлам[3].

Ограничение прав доступа играет ключевую роль в обеспечении безопасности временных файлов. Настройка системы таким образом, чтобы временные файлы были доступны только для процессов СУБД, предотвращает их просмотр и модификацию со стороны других приложений или пользователей. Помимо этого, важно использовать сегментацию сети, чтобы отделить сервер баз данных от других элементов инфраструктуры, минимизируя риск прямого доступа к файловой системе[4].

Ещё одним способом уменьшения зависимости от временных файлов является оптимизация SQL-запросов. Хорошо спроектированный запрос, например, с использованием индексов, может значительно сократить необходимость создания временных таблиц и файлов. Это не только повышает производительность системы, но и снижает вероятность утечки данных. Кроме того, администраторы баз данных могут настроить ограничение на размер временных файлов и их время хранения, чтобы уменьшить вероятность их использования злоумышленниками.

Не менее важен мониторинг работы системы. Инструменты для анализа активности файловой системы могут помочь обнаружить подозрительные действия, связанные с временными файлами, такие как их внезапное увеличение в объёме или попытки доступа со стороны непривилегированных процессов. В сочетании с журналированием событий в СУБД это позволяет администратору оперативно реагировать на возможные инциденты безопасности[5].

В современных условиях также стоит рассмотреть использование облачных решений, где временные файлы обрабатываются на виртуализированных и защищённых платформах.

Такие платформы часто предоставляют встроенные механизмы защиты, включая шифрование данных в режиме реального времени и автоматическое удаление временных файлов после завершения операций. Однако и здесь не стоит полагаться исключительно на поставщиков облачных услуг — необходимо проводить регулярные аудиты безопасности и следить за правильной настройкой системы

Заключение

Минимизация временных файлов и защита их содержимого являются важными аспектами управления безопасностью базы данных. Несмотря на то, что временные файлы играют важную роль в производительности СУБД, они остаются одной из наиболее уязвимых точек для утечки данных. Использование шифрования, настройка прав доступа, оптимизация запросов и мониторинг активности системы — всё это ключевые меры, которые помогают значительно снизить риск утечки через временные файлы.

С ростом объёмов данных и усложнением архитектуры современных систем управление безопасностью становится ещё более критичным. Органы, обрабатывающие конфиденциальную информацию, включая финансовые учреждения и медицинские организации, особенно уязвимы перед угрозами утечек. Поэтому внедрение лучших практик, таких как многоуровневая защита данных и регулярные аудиты безопасности, становится обязательным условием для предотвращения утечек через временные файлы.

Интеграция автоматизированных инструментов защиты и настройка политики безопасности позволяют создать надёжную защиту от современных угроз. В конечном итоге, эффективная защита временных файлов — это не только технический, но и организационный процесс, который требует постоянного внимания и обновления.

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. Шемякин С. Н., Ахметшина М. Э., Катасонов А. И. Поиск функций, обладающих наилучшими характеристиками в классе от 4 переменных //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 61-65.
3. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
4. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
5. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.

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 space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
2. Shemyakin S. N., Akhmetshina M. E., Katasonov A. I. Search for functions with the best characteristics in a class of 4 variables //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 61-65.
3. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
4. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
5. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 653-657.