Пивоварова У.А. PAPERCUT: уязвимость CVE-2023-27350 и ее последствия для корпоративной безопасности // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 11(49) с. 29–32

Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056

PAPERCUT: УЯЗВИМОСТЬ CVE-2023-27350 И ЕЕ ПОСЛЕДСТВИЯ ДЛЯ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

Пивоварова У.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: pivovarova.ulyana2017@yandex.ru

В данной статье рассматривается критическая уязвимость CVE-2023-27350 в популярном ПО для управления печатью PaperCut. Подробно анализируются природа уязвимости, способы ее эксплуатации злоумышленниками и возможные последствия для корпоративных сетей. Также представлены рекомендации по защите и устранению уязвимости, чтобы минимизировать риски для организаций.

Ключевые слова: PaperCut, CVE-2023-27350, уязвимость, кибербезопасность, управление печатью, защита данных, корпоративная безопасность, эксплуатация уязвимостей, обновления безопасности.

PAPERCUT: VULNERABILITY CVE-2023-27350 AND ITS IMPLICATIONS FOR CORPORATE SECURITY

Pivovarova U.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: pivovarova.ulyana2017@yandex.ru

This article explores the critical vulnerability CVE-2023-27350 in the widely used print management software PaperCut. It provides a detailed analysis of the vulnerability, methods of exploitation by attackers, and the potential consequences for corporate networks. Additionally, the article offers recommendations on how to mitigate the risk and patch the vulnerability to protect organizations.

Keywords: PaperCut, CVE-2023-27350, vulnerability, cybersecurity, print management, data protection, corporate security, vulnerability exploitation, security updates.

Введение

Современные компании активно используют специализированное программное обеспечение для управления печатью, и одним из популярных решений является PaperCut. Однако в начале 2023 года стало известно о критической уязвимости в этой системе — CVE-2023-27350. Эта уязвимость вызвала большой резонанс в киберсообществе, так как позволяет злоумышленникам получить несанкционированный доступ к системе, а в некоторых случаях — полный контроль над корпоративными сетями. В данной статье мы рассмотрим природу уязвимости, как она может быть использована, какие риски несет для компаний и как можно защититься от подобных угроз.

Природа уязвимости CVE-2023-27350

CVE-2023-27350 относится к категории удалённых уязвимостей, позволяющих злоумышленникам получить доступ к серверу PaperCut без аутентификации. Уязвимость была обнаружена в механизме авторизации PaperCut, что позволило злоумышленникам выполнять произвольный код на сервере, получая контроль над печатными заданиями и другими внутренними ресурсами компании.

Одной из самых опасных сторон этой уязвимости является её относительно простая эксплуатация. Злоумышленнику не требуется сложных инструментов или глубоких знаний о внутренней архитектуре PaperCut. В некоторых случаях атака может быть проведена с использованием обычного удалённого доступа, а её последствия могут быть разрушительными — от утечки данных до полной остановки работы предприятия[2].

Способы эксплуатации уязвимости

Злоумышленники могут использовать CVE-2023-27350 для различных целей. Среди них:

Удалённое выполнение кода (RCE): злоумышленник может внедрить и запустить произвольные программы на сервере PaperCut, что может привести к компрометации всей системы[1].

Управление печатными заданиями: контроль над заданиями на печать может привести к утечке конфиденциальной информации, что особенно опасно для компаний, работающих с документами высокой важности.

Распространение вредоносного ПО: через сервер PaperCut злоумышленники могут внедрить вирусы или шпионское ПО в корпоративную сеть, что может вызвать массовое заражение устройств.

Последствия для корпоративной безопасности

Уязвимость CVE-2023-27350 представляет собой серьёзную угрозу для компаний, использующих PaperCut в своей инфраструктуре. В первую очередь, это риск утечки конфиденциальных данных. В условиях цифровой трансформации, когда печатные документы могут содержать важные финансовые отчёты, юридические документы и личные данные клиентов, утечка такой информации может привести к значительным финансовым и репутационным потерям[3].

Кроме того, компрометация системы печати может быть использована как стартовая точка для более масштабных атак на корпоративную сеть. После получения контроля над сервером PaperCut, злоумышленник может использовать его для дальнейшего проникновения в сеть, взлома других систем или даже полного отключения корпоративных сервисов.

Рекомендации по защите

Чтобы минимизировать риски, связанные с CVE-2023-27350, рекомендуется принять следующие меры:

Обновление ПО: первое и самое важное действие — обновить PaperCut до последней версии, где данная уязвимость закрыта[4].

Мониторинг сетевой активности: регулярный анализ логов серверов PaperCut может помочь вовремя выявить подозрительную активность.

Ограничение доступа: ограничьте доступ к серверу PaperCut только доверенным пользователям и устройствам. Используйте двухфакторную аутентификацию для дополнительной защиты.

Сегментация сети: разделение сети на сегменты ограничит возможности злоумышленников в случае взлома одной из систем[5].

Заключение

CVE-2023-27350 стала очередным напоминанием о важности постоянного мониторинга и обновления программного обеспечения. Уязвимости в таких ключевых системах, как PaperCut, могут представлять серьёзную угрозу для безопасности данных и всей корпоративной инфраструктуры. Организациям следует не только своевременно обновлять свои системы, но и внедрять более строгие меры безопасности, чтобы минимизировать возможные риски. В условиях роста кибератак каждый новый уязвимый компонент может стать входной точкой для злоумышленников, поэтому компании должны быть максимально подготовлены к подобным вызовам.

Список литературы

1. 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.
2. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

References

1. Bogomaz M. E., Mikhailova L. A., Polyanicheva A. V. TOOLS FOR ENSURING THE SECURITY OF IP TELEPHONY // Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 170-172.
2. Volkogonov V. N. et al. Application of Physical Non-Cloning Functions for Authentication in the Internet of Things Environment. – 2021. – pp.409-414.
3. Sinelshchikov V. S., Tsvetkov A. Y. Zashchita lichnykh dannykh na predpriyatiye [Protection of personal data at the enterprise]. – 2021. – pp. 653-657.
4. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data. – 2018. – pp. 236-240.

5. Kushnir D. V. Research and development of methods for the distribution of confidential data on quantum channels. –Saint Petersburg. State University of Telecommunications named after MA Bonch-Bruevich, 1996.