Международный журнал информационных технологий и энергоэффективности

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

УДК 004.056.55

КРИТИЧЕСКАЯ УЯЗВИМОСТЬ - CVE-2023-27350

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

В данной статье рассматривается уязвимость CVE-2023-27350, обнаруженная в приложении PaperCut NG/MF, широко используемом для управления процессами печати в крупных организациях. Особое внимание уделяется резкому росту числа атак, связанных с этой уязвимостью, что обусловлено её характером как zero-click эксплойта, не требующего взаимодействия пользователя и позволяющего полностью автоматизировать доставку вредоносного ПО. В статье подробно объясняется механизм уязвимости, показаны методы её эксплуатации, предлагаются стратегии защиты, а также подчеркивается важность соблюдения принципов безопасности, включая необходимость тщательной очистки после установки программного обеспечения.

Ключевые слова: CVE-2023-27350, zero-click эксплойт, автоматизация, доставка вредоносного ПО, защита, очистка после установки, уязвимость, безопасность.

CRITICAL VULNERABILITY - CVE-2023-27350

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

This article examines the vulnerability CVE-2023-27350, discovered in the PaperCut NG/MF application, widely used to manage printing processes in large organizations. Particular attention is paid to the sharp increase in the number of attacks related to this vulnerability, due to its nature as a zero-click exploit that does not require user interaction and allows for fully automated malware delivery. The article explains in detail the mechanism of the vulnerability, shows methods of its exploitation, suggests protection strategies, and emphasizes the importance of following security principles, including the need for thorough cleaning after installing software.

Keywords: CVE-2023-27350, zero-click exploit, automation, malware delivery, protection, post-installation cleanup, vulnerability, security.

Введение

8 марта 2023 года был выпущен патч для уязвимости CVE-2023-27350, которая обнаружена в приложении PaperCut NG/MF — веб-ориентированном программном обеспечении, используемом крупными организациями для управления процессами печати. Уязвимость позволяет злоумышленникам удаленно получить административный доступ к веб-приложению и использовать легитимную функциональность скриптов для выполнения кода на сервере с правами SYSTEM.

Однако, в последующие месяцы была зафиксирована активная эксплуатация этой уязвимости в дикой природе. Количество атак увеличивается, включая доставку вредоносного ПО с использованием C2-фреймворков, таких как CobaltStrike, и даже программ-вымогателей.

Среди групп, стоящих за активной эксплуатацией, фигурируют известные APT-группы, включая Cl0p.

Стремительное увеличение числа атак, связанных с уязвимостью CVE-2023-27350, вызвано её природой как zero-click эксплойта, не требующего взаимодействия пользователя. Этот тип уязвимости позволяет злоумышленникам полностью автоматизировать процесс доставки вредоносного ПО на уязвимые системы. В данном руководстве мы подробно разберем природу этой уязвимости, продемонстрируем её возможные методы эксплуатации, предложим меры защиты и обсудим основополагающий принцип безопасности, напомнивший нам об актуальности темы — необходимость тщательной очистки после установки программного обеспечения.

Paper cut

PaperCut — это популярное программное обеспечение для управления печатью, которое используется организациями по всему миру для контроля и управления услугами печати и копирования. В линейке продуктов PaperCut предлагаются два схожих решения, размещаемых на собственных серверах:

PaperCut NG — решение для управления и контроля процессов печати.

PaperCut MF — аналогичный продукт, но с расширенными функциями копирования и сканирования[2].

Компания PaperCut объявила, что не обновленные серверы MF и NG активно подвергаются атакам, так как они уязвимы к обходу аутентификации, описанному ниже.

CVE-2023-27350

Инициатива Zero Day (ZDI-23-233) описывает CVE-2023-27350 как уязвимость, которая позволяет неаутентифицированному удаленному злоумышленнику выполнить произвольный код и скомпрометировать сервер приложения PaperCut. Эта уязвимость также напрямую связана с CVE-2023-27351, которая, используя ту же самую уязвимость, описанную ниже, позволяет злоумышленнику извлекать информацию (имена пользователей, электронные почты и хэши паролей) из базы данных пользователей, хранящейся в PaperCut[5].

Эта уязвимость имеет два аспекта и изначально возникает из-за уязвимости обхода аутентификации. Это позволяет неаутентифицированному удаленному злоумышленнику обойти страницу входа и получить административный доступ к консоли PaperCut, просто сделав запрос к URL, который изначально использовался в процессе установки приложения.

Этот запрос инициирует класс SetupCompleted, который, как показано в приведенном ниже блоке кода, включает вызов метода Java performLogin(), передавая аргумент Admin в качестве параметра LoginType.

Приложение обычно вызывает эту функцию только после того, как пользователь успешно прошел проверку в процессе обычного входа в систему. Однако в данном случае присутствует уязвимость типа Session Puzzling в классе SetupCompleted — логическая уязвимость, возникающая, когда функции сессии и аутентификации используются для разных целей. Эксплуатируя эту уязвимость, приложение ошибочно подтверждает сессию администратора для неаутентифицированного пользователя.

Этот обход аутентификации приводит к удаленному выполнению кода путем злоупотребления встроенной функцией "скриптинга" в консоли администратора. Если уязвимость будет использована, злоумышленник может вставить произвольный JavaScript в

скрипт шаблона печати. Отключение параметра конфигурации песочницы дает скриптам прямой доступ к среде выполнения Java, что позволяет выполнить произвольный код. Код может быть выполнен по требованию, просто сохранив скрипт[4]. Таким образом, простое редактирование скрипта может привести к удаленному выполнению кода.

Ситуацию усугубляет то, что выполненные скрипты работают в контексте службы PrintCut, которая, в свою очередь, выполняется с полными привилегиями учетной записи NT AUTHORITY\SYSTEM в Windows (или учетной записи root в Linux). Таким образом, использование этой уязвимости предоставляет ранее неаутентифицированному злоумышленнику полный контроль над хостом[1]!

Влияние

Серьезность уязвимости CVE-2023-27350 проявилась в многочисленных случаях её активной эксплуатации злоумышленниками, которые использовали её для автоматизированных атак на целевые системы. После публикации PoC-эксплойта исследователи отметили массовые атаки на уязвимые серверы по всему миру, особенно в образовательном секторе, с участием таких группировок, как Cl0p. Поиск в Shodan в апреле 2023 года показал около 1 700 серверов PaperCut, доступных через интернет, что делает их привлекательными для атак. Злоумышленники также использовали легитимные инструменты ИТ-специалистов и такие угрозы, как Truebot, Buhtiransom, Mirai и майнеры криптовалют[3].

Заключение

В этой статье мы рассказали, насколько легко использовать уязвимость обхода аутентификации в PaperCut и злоупотребить функцией скриптов для достижения удаленного выполнения кода. Стоит отметить, что поскольку выполнение кода происходит через легитимную функцию, даже если вы установили патч для этой уязвимости, злоумышленники все равно могут воспользоваться ею, если вы настроили слабый пароль в приложении.

Список литературы

1. Гельфанд А. М. Способы выбора стегоконтейнеров для передачи данных //Региональная информатика и информационная безопасность. – 2020. – С. 260-262
2. 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.
3. 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.
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. Петрова Т. В. и др. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети //Региональная информатика (РИ-2022). – 2022. – С. 572-573.

References

1. Gelfand A.M. Methods of choosing stegocontainers for data transmission //Regional informatics and information security. - 2020. – pp. 260-262
2. Kushnir D. V. Research and development of methods for distributing confidential data via quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
3. Lesnova E. M., Pestov I. E. Development of a method for detecting and correcting errors for a distributed information network based on big data //Regional informatics and information security. - 2018. – pp. 236-240.
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. Petrova T. V. et al. Approaches for detecting an attacker's wireless access point on a local computer network //Regional Informatics (RI-2022). – 2022. – pp. 572-573.