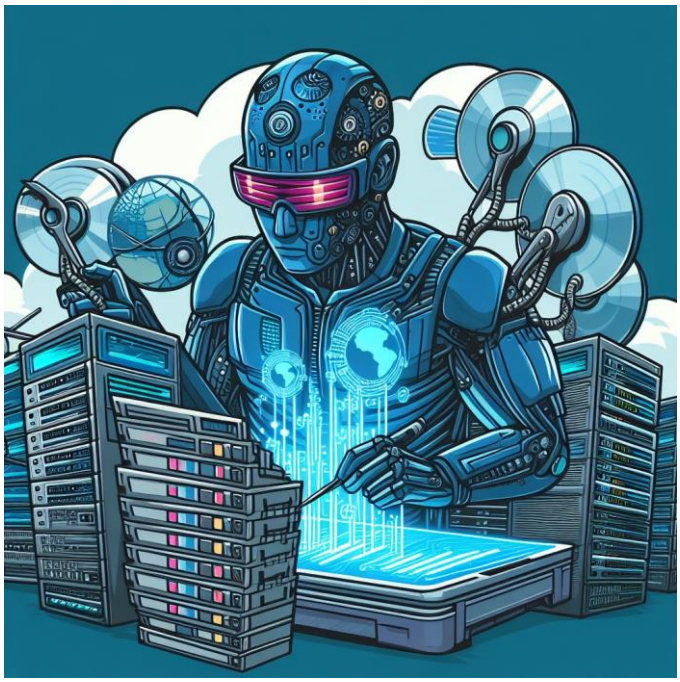

Аннотация – В этом документе представлен анализ уязвимости CVE-2023–22518, связанной с неправильной авторизацией в Atlassian Confluence Data Center and Server. Анализ будет охватывать различные аспекты уязвимости, включая её обнаружение, воздействие, методы эксплуатации и стратегии смягчения последствий.

Специалисты по безопасности найдут этот анализ особенно полезным, поскольку он предоставляет оперативную информацию, включая показатели компрометации и подробные шаги по смягчению последствий. Понимая первопричины, методы эксплуатации и эффективные контрмеры, эксперты по безопасности могут лучше защитить свои организации от подобных угроз в будущем.

I. Введение

CVE-2023-22518 – уязвимость неправильной авторизации, которая затрагивает все версии Confluence Data Center. Эта уязвимость позволяет злоумышленнику, не прошедшему проверку подлинности, перезагрузить Confluence и получить контроль над уязвимой системой.

Изначально уязвимости был присвоен критический балл серьёзности 9,1 в CVSS, но позже он был повышен до 10, что является наивысшим показателем критичности, из-за изменения масштаба атаки и наблюдения за активными эксплойтами и сообщениями об исполнителях угроз, использующих программы-вымогатели.

Atlassian выпустила исправленные версии Confluence для решения CVE-2023-22518. Исправленными версиями являются 7.19.16, 8.3.4, 8.4.4, 8.5.3 и 8.6.1. Кроме того, рекомендуется ограничить внешний доступ к серверам Confluence до тех пор, пока не будет применено обновление. Эта уязвимость не затрагивает пользователей Atlassian Cloud.

II. Подробности атак

Уязвимость была обнаружена из-за разницы в исправлениях между исправленной и не исправленной версиями ПО и заключается в конечных точках "восстановления настроек" в экземплярах Confluence, которые были доступны пользователям, не прошедшим проверку подлинности. Конечные точки являются частью функций восстановления системы и предназначены для использования администраторами для восстановления экземпляра Confluence из резервной копии. Конечные точки, к которым должен иметь доступ только пользователь-администратор, включают /json/setup-restore.action, /json/setup-restore-local.action и /json/setup-restore-progress.action. Используя их, возможно загрузить специально созданный zip-архивный файл через HTTP Post-запрос. Zip-файл может содержать веб-шелл для выполнения произвольных команд.

A. Схема атаки

Процесс атаки CVE-2023–22518 включает в себя несколько этапов, которые позволяют злоумышленнику, не прошедшему проверку подлинности, использовать уязвимости неправильной авторизации:

- **Использование параметров "Восстановления настроек"**: конечные точки "setup restore" в Confluence предназначены для администраторов для восстановления экземпляра Confluence из резервной копии. Из-за уязвимости эти конечные точки доступны для не прошедших проверку подлинности пользователей
- **Загрузка вредоносного zip-файла**: злоумышленник создаёт специально разработанный zip-файл, который при загрузке на уязвимый сервер Confluence через скомпрометированные конечные точки может либо уничтожить экземпляр Confluence, что приведёт к потере данных, либо содержать веб-шелл для удалённого выполнения кода (RCE) на сервере
- **Получение несанкционированного доступа**: если атака включает загрузку веб-шелла, злоумышленник может выполнять произвольные команды на сервере. Этот уровень доступа позволяет злоумышленнику выполнять все административные действия, доступные администраторам экземпляра Confluence, эффективно получая контроль над системой
- **Развёртывание программ-вымогателей**: в некоторых случаях злоумышленники использовали эту уязвимость для развёртывания программ-вымогателей, таких как Cerber ransomware. При запуске программа-вымогатель шифрует файлы на локальных дисках и общих сетевых ресурсах, добавляя к зашифрованным файлам определённое расширение файла (например, LOCK3D) и требует выкуп за расшифровку данных
- **Последствия**: Успешное использование CVE-2023–22518 может привести к несанкционированному управлению системой, потере данных, сбоям в работе и финансовым затратам из-за развёртывания программ-вымогателей, нарушения работы, получения доступа к конфиденциальной информации, а также манипулированию данными или их удалению.

B. PoC

exploit.py выполняет следующие действия (GitHub https://github.com/ForceFledgling/CVE-2023-22518):

- **Идентификация цели**: скрипт предложит ввести URL уязвимого экземпляра Confluence.
- **Выполнение эксплойта**: затем скрипт использует предоставленный URL-адрес для отправки обработанных запросов точкам "setup restore", таким как /json/setup-restore.action, которые обычно доступны только администраторам, но в уязвимых версиях – обычным пользователям, не прошедшим проверку подлинности, из-за уязвимости.
- **Загрузка вредоносной полезной нагрузки**: эксплойт включает загрузку вредоносного zip-файла, который может содержать веб-шелл или другой вредоносный код, на сервер через скомпрометированные конечные точки.
- **Удалённое выполнение кода (RCE)**: если загруженный zip-файл содержит веб-шелл, злоумышленник может выполнять произвольные команды на сервере, что приведёт к несанкционированному управлению системой.
- **Результат**: административный доступ к экземпляру Confluence, который может быть использован для выполнения дальнейших вредоносных действий, таких как эксфильтрация данных, уничтожение данных или развёртывание программ-вымогателей.

Входящие данные для скрипта будут включать URL целевого экземпляра Confluence и путь к вредоносному zip-файлу. Исходящие данные будут состоять из HTTP-запросов к уязвимым конечным точкам и потенциально загруженной вредоносной полезной нагрузки.

xmlexport-20231109-060519-1.zip – файл предназначен для загрузки в уязвимый Confluence и экземпляр сервера для использования уязвимости неправильной авторизации. При загрузке в уязвимый экземпляр Confluence это может привести к несанкционированной загрузке файлов, потенциально позволяя удалённое выполнение кода или другие уязвимости в системе безопасности.

CVE-2023–22518 в контексте использования файла .jar, например **atlplug.jar** может служить в качестве приложения-бэкдора Confluence для выполнения определённых действий на уязвимом сервере Confluence.

III. Отрасли

Atlassian Confluence используется в ряде отраслей промышленности благодаря своей универсальности в качестве ПО для командной работы:

- **Информационные технологии и услуги**: Confluence широко используется в ИТ-секторе для управления знаниями, документации и совместной работы над проектами по разработке ПО
- **Программное обеспечение**: компании-разработчики ПО используют Confluence для управления документацией по своему продукту, отслеживания прогресса проекта и облегчения общения между членами команды
- **Финансовые услуги**: Финансовая индустрия использует Confluence для систематизации конфиденциальной информации, ведения документации по соблюдению нормативных требований и поддержки внутреннего делопроизводства
- **Образование**: Образовательные учреждения могут использовать Confluence в качестве базы знаний для ИТ-поддержки, а также для управления образовательными материалами и исследованиями и совместного использования с ними
- **Госсектор**: Госучреждения могут использовать Confluence для управления проектами, документацией и создания централизованного хранилища институциональных знаний
- **Здравоохранение**: Организации здравоохранения могут использовать Confluence для управления информационными системами пациентов, документацией исследований и в качестве базы знаний для медицинского персонала

A. Воздействие

Эксплуатация CVE-2023–22518 может привести к:

- **Несанкционированный контроль системы**: Злоумышленники могут получить административный доступ, позволяющий им выполнять любые действия внутри экземпляра Confluence, которые могут нарушить работу и поставить под угрозу конфиденциальные данные
- **Развёртывание программы-вымогателя**: были случаи, когда уязвимость использовалась для развёртывания программы-вымогателя Cerber, что приводило к шифрованию данных и требованиям выкупа, что могло остановить ИТ-операции и привести к финансовым потерям
- **Сбой в работе**: Сброс экземпляра Confluence может нарушить текущие проекты и усилия по совместной работе, что приведёт к задержкам и потенциальной потере данных

B. Последствия

- **Потеря данных**: несанкционированный доступ и потенциальное внедрение программ-вымогателей могут привести к необратимой потере данных, что особенно опасно в отрасли, которая полагается на целостность данных
- **Финансовые затраты**: Затраты, связанные с запросами программ-вымогателей, восстановлением системы и потенциальными штрафами регулирующих органов, могут быть существенными
- **Ущерб репутации**: Нарушения безопасности могут нанести ущерб репутации поставщиков ИТ-услуг, что приведёт к потере доверия и потенциальной потере бизнеса
- **Перераспределение ресурсов**: ИТ-отделам может потребоваться перенаправление ресурсов для устранения уязвимости и её последствий, что может отвлечь внимание от других важных ИТ-инициатив