Хакеры начали эксплуатировать уязвимость в считанные часы после раскрытия.

Новая критическая уязвимость в MOVEit Transfer — это программное обеспечение для управления передачей файлов, разработанное Ipswitch, дочерней компанией Progress Software. Оно предназначено для безопасной и надежной передачи файлов между различными системами, включая серверы, облачные платформы и другие внешние устройства.

 MOVEit Transfer обеспечивает шифрование данных, контроль доступа и аудит передачи файлов, что обеспечивает высокий уровень безопасности. ПО позволяет организациям передавать файлы любого размера и типа, а также контролировать, кто и когда имеет доступ к передаваемым данным." data-html="true" data-original-title="MOVEit Transfer" >MOVEit Transfer от Progress Software Corporation — американская компания, специализирующаяся на разработке программного обеспечения и предоставлении инструментов для разработки и управления бизнес-приложениями.

 Компания была основана в 1981 году и предлагает широкий спектр продуктов, включая инструменты для разработки приложений, базы данных, интеграции данных и аналитических решений." data-html="true" data-original-title="Progress Software" >Progress Software позволяет кибератакам обходить механизмы аутентификации платформы. В течение нескольких часов после публикации информация об уязвимости начала активно эксплуатироваться в реальных условиях.

MOVEit Transfer — это приложение для обмена файлами и сотрудничества в крупных предприятиях. В прошлом году оно стало мишенью вымогательской группировки Cl0p, атака которой затронула как минимум 160 жертв.

Новая уязвимость (CVE-2024-5806, CVSS: 7.4) является проблемой ненадлежащей аутентификации в модуле SFTP MOVEit. По данным Progress, она «может привести к обходу аутентификации в ограниченных сценариях». Уязвимость затрагивает версии MOVEit Transfer с 2023.0.0 по 2023.0.11, с 2023.1.0 по 2023.1.6 и с 2024.0.0 по 2024.0.2

Администраторам рекомендуется немедленно установить исправления. После прошлогодних атак MOVEit находится под пристальным вниманием киберпреступников, и доступ к внутренним файлам компаний из списка Fortune 1000 является весьма привлекательной целью для шпионских угроз.

По данным сервиса Shadowserver, вскоре после публикации информации об уязвимости специалисты начали наблюдать попытки эксплуатации CVE-2024-5806 в Progress MOVEit Transfer через POST «/guestaccess.aspx». Сообщается, что в сети доступно по меньшей мере 1800 экземпляров MOVEit, хотя не все из них уязвимы.

Progress не предоставил подробностей о проблеме, но исследователи из watchTowr определили два сценария атаки. В одном случае злоумышленник может провести «принудительную аутентификацию» с использованием вредоносного SMB-сервера и действительного имени пользователя. В более опасном сценарии злоумышленник может выдать себя за любого пользователя системы.

Исследователи из watchTowr пояснили: «Мы можем загрузить наш SSH-ключ на сервер без входа в систему и затем использовать этот ключ для аутентификации от имени любого пользователя. Таким образом, мы получаем доступ ко всем функциям пользователя, включая чтение, изменение и удаление защищённых данных».