НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза несанкционированного доступа к облачному хранилищу ownCloud

ALRT-20231128.1 | 28 ноября 2023 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Описание угрозы	По каналам НКЦКИ получены сведения о критических уязвимостях в программном обеспечении ownCloud, которое предназначено для синхронизации данных и совместной работы с файлами. Уязвимость CVE-2023-49103 содержится в приложении Graph API в версиях 0.2.0 – 0.3.0. Ее эксплуатация позволяет злоумышленнику получить доступ к конфиденциальным данным в целевой системе с помощью URL-адреса сторонней библиотеки (GetPhpInfo.php) приложения Graph API. При доступе к этому URL-адресу раскрывается конфигурация среды PHP, включая критические переменные среды веб-сервиса, такие как пароль администратора ownCloud, учетные данные почтового сервера и лицензионный ключ. Вторая уязвимость CVE-2023-49105 была обнаружена в библиотеках ядра ownCloud в версиях 10.6.0 – 10.13.0. Эксплуатация данной уязвимости позволяет злоумышленнику получить доступ к целевой системе, модифицировать или удалить любой файл в уязвимом приложении посредством обхода аутентификации в API WebDAV, если известно имя пользователя и у него не настроен ключ подписи (по умолчанию он не настроен). Третья уязвимость CVE-2023-49104 затрагивает приложение Oauth2. Ее эксплуатация позволяет злоумышленнику перенаправлять ответы на подконтрольный ему домен посредством ввода специально созданного URL-адреса. В целях минимизации возможных рисков необходимо обновить программное обеспечение ownCloud и принять меры, разработанные официальным вендором, которые представлены ниже.
Рекомендации	В приложении Graph API: - удалить файл owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php; - сменить потенциально скомпрометированные аутентификационные данные, включая пароль администратора ownCloud, учетные данные от почтового сервера, БД и ключи доступа для Object-Store/S3. Для компонента API WebDAV следует установить запрет на использование pre-signed URL, если для владельца файлов не настроен ключ подписи, а также необходимо настроить ключи подписи для всех пользователей. Если невозможно в данный момент выполнить обновление, необходимо осуществить следующие действия: - удалить файл owncloud/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php; - отключить функцию phpinfo в контейнерах Docker; - в приложении Oauth2 необходимо отключить опцию Allow Subdomains; - в API WebDAV необходимо настроить ключи подписи для всех пользователей, а также установить запрет на использование pre-signed URL, если для владельца файлов не настроен ключ подписи.