# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211102.2 | 2 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Перезапись произвольных файлов в Nextcloud Server

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2021-32610 |
| Идентификатор программной ошибки | CWE-59: Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке") |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику перезаписать произвольные файлы в целевой системе. Уязвимость обусловлена некорректной проверкой файла в архиве. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Nextcloud Server: 20.0.0, 20.0.1, 20.0.2, 20.0.3, 20.0.4, 20.0.5, 20.0.6, 20.0.7, 20.0.8, 20.0.9, 20.0.10, 20.0.11, 20.0.12, 21.0.0, 21.0.1, 21.0.2, 21.0.3, 21.0.4, 22.0.0, 22.1.0, 22.1.1 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 20 июля 2021 г. |
| Дата обновления | 22 июля 2021 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| Вектор атаки (AV) | Сетевой (N) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Отсутствует (N) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |
| Влияние на конфиденциальность (C) | Высокое (H) |

| | |
|---|---|
| Влияние на целостность (I) | Высокое (H) |
| Влияние на доступность (A) | Высокое (H) |
| Степень зрелости доступных средств эксплуатации | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2021102617<br>http://github.com/pear/Archive_Tar/releases/tag/1.4.14 |