# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220430.13 | 30 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

## Загрузка вредоносного файла в TYPO3

| | |
|---|---|
| Идентификатор уязвимости | Не определен |
| Идентификатор программной ошибки | CWE-434: Отсутствие ограничений на загрузку файлов небезопасного типа |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и выполнить вредоносный файл на уязвимом сервере. Уязвимость обусловлена некорректной проверкой файла во время загрузки. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Job portal: 3.0.0 |
| Рекомендации по устранению | Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. |
| Дата выявления | 26 апреля 2022 г. |
| Дата обновления | 26 апреля 2022 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C |
| 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 | Не изменяется (U) |

| | |
|---|---|
| уязвимости (S) | |
| 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 | http://typo3.org/security/advisory/typo3-ext-sa-2022-005/ |