

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210915.8 | 15 сентября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Adobe Photoshop

|                                                   |                                                                                                                                                                                                                                     |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Идентификатор уязвимости                          | MITRE: CVE-2021-40709                                                                                                                                                                                                               |
| Идентификатор программной ошибки                  | CWE-119: Выполнение операций за пределами буфера памяти                                                                                                                                                                             |
| Описание уязвимости                               | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. |
| Категория уязвимого продукта                      | Прикладное программное обеспечение                                                                                                                                                                                                  |
| Уязвимый продукт                                  | Adobe Photoshop: 21.0.1, 21.0.2, 21.1, 21.1.1, 21.2, 21.2.1, 21.2.2, 21.2.3, 21.2.4, 21.2.5, 21.2.6, 21.2.7, 21.2.8, 21.2.9, 21.2.10, 21.2.11, 22.1.0, 22.1.1, 22.2, 22.3, 22.3.1, 22.4, 22.4.1, 22.4.2, 22.4.3, 22.5               |
| Рекомендации по устранению                        | Обновить программное обеспечение                                                                                                                                                                                                    |
| Дата выявления                                    | 15 сентября 2021 г.                                                                                                                                                                                                                 |
| Дата обновления                                   | 15 сентября 2021 г.                                                                                                                                                                                                                 |
| Оценка критичности уязвимости (CVSSv3.1)          | 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N                                                                                                                                                                                             |
| Вектор атаки (AV)                                 | Сетевой (N)                                                                                                                                                                                                                         |
| Сложность эксплуатации уязвимости (AC)            | Низкая (L)                                                                                                                                                                                                                          |
| Необходимый уровень привилегий (PR)               | Отсутствует (N)                                                                                                                                                                                                                     |
| Необходимость взаимодействия с пользователем (UI) | Требуется (R)                                                                                                                                                                                                                       |
| 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/SB2021091501>  
<https://helpx.adobe.com/security/products/photoshop/apsb21-84.html>