

# 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-20210322.6 | 22 марта 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольных команд оболочки в Creative Cloud Desktop Application

|   |  |
|---|--|
| Идентификатор уязвимости                          | MITRE: CVE-2021-21078  |
| Идентификатор программной ошибки                  | CWE-78: Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)  |
| Описание уязвимости                               | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных. |
| Категория уязвимого продукта                      | Универсальные библиотеки и компоненты  |
| Уязвимый продукт                                  | Creative Cloud Desktop Application:5.1.0.407, 5.2.0.436, 5.2.1.441, 5.3.1.470, 5.3.5.499, 5.3.5.518  |
| Рекомендации по устранению                        | Обновить программное обеспечение   |
| Дата выявления                                    | 10 марта 2021 г.   |
| Дата обновления                                   | 10 марта 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                             | <a href="https://www.cybersecurity-help.cz/vdb/SB2021031002">https://www.cybersecurity-help.cz/vdb/SB2021031002</a><br><a href="https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html">https://helpx.adobe.com/security/products/creative-cloud/apsb21-18.html</a> |