

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201027.6 | 27 октября 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Creative Cloud Desktop Application

| | |
|---|--|
| Идентификатор уязвимости | MITRE: CVE-2020-24422 |
| Идентификатор программной ошибки | CWE-426: Подмена пути исполнения |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой пути поиска. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Creative Cloud Desktop Application: old installer до v5.2, new installer до v2.1 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 21 октября 2020 г. |
| Дата обновления | 21 октября 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 9.8 AV:N/AC:L/PR:N/UI:N/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) | 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://helpx.adobe.com/security/products/creative-cloud/apsb20-68.html https://www.cybersecurity-help.cz/vdb/SB2020102121 |