

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230315.4 | 15 марта 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Creative Cloud Desktop Application

Идентификатор уязвимости	MITRE: CVE-2023-26358
Идентификатор программной ошибки	CWE-427: Неконтролируемый элемент пути поиска
Описание уязвимости	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной загрузкой исполняемых файлов.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Creative Cloud Desktop Application: 5.0 - 5.9.1
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	14 марта 2023 г.
Дата обновления	14 марта 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	8.6 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)

Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено

Ссылки на источники

<http://helpx.adobe.com/security/products/creative-cloud/apsb23-21.html>