

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211102.9 | 2 ноября 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Adobe Media Encoder

Идентификатор уязвимости	MITRE: CVE-2021-43013 CVE-2021-40777 CVE-2021-40779 CVE-2021-40780
Идентификатор программной ошибки	CWE-788: Доступ к областям памяти за пределами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти при обработке входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Media Encoder: 12.0, 12.0.1, 12.1, 12.1.1, 12.1.2, 13.0, 13.0.1, 13.0.2, 13.1, 13.1.3, 13.1.5, 14.0, 14.0.1, 14.0.2, 14.1, 14.2, 14.3, 14.3.2, 14.4, 14.5, 14.6, 15.0, 15.1, 15.2, 15.3, 15.4, 15.4.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	1 ноября 2021 г.
Дата обновления	1 ноября 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/SB2021110104>
<http://helpx.adobe.com/security/products/media-encoder/apsb21-99.html>