НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200618.3 | 18 июня 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Adobe After Effects

Идентификатор уязвимости	MITRE: CVE-2020-9661 CVE-2020-9660 CVE-2020-9662 CVE-2020-9637 CVE-2020-9638
Идентификатор программной ошибки	CWE-125: Чтение за пределами буфера CWE-787: Запись за границами буфера CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена переполнением буфера памяти при обработке входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Adobe After Effects до v17.1.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 июня 2020 г.
Дата обновления	16 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/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)	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/SB2020061615 https://helpx.adobe.com/security/products/after_effects/apsb20-35.html