

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201223.7 | 23 декабря 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в ПО Adobe

Идентификатор уязвимости	MITRE: CVE-2020-24440 CVE-2020-24447
Идентификатор программной ошибки	CWE-427: Неконтролируемый элемент пути поиска
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного DLL-файла. Уязвимость обусловлена некорректной загрузкой DLL-библиотек.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Lightroom: 8.0, 8.1, 8.2, 8.3, 8.4, 9.0, 9.2, 9.2.0.10, 9.3, 10.0 Prelude: 7.0, 7.0.1, 7.1, 7.1.1, 8.0, 8.0.1, 8.1, 8.1.1, 9.0, 9.0.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 декабря 2020 г.
Дата обновления	8 декабря 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/SB2020120851 https://helpx.adobe.com/security/products/prelude/apsb20-70.html https://helpx.adobe.com/security/products/lightroom/apsb20-74.html