

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210216.5 | 16 февраля 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости	MITRE: CVE-2021-21051 CVE-2021-21048
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена переполнением буфера при некорректной обработке файлов Photoshop.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Photoshop: 19.0, 19.1, 19.1.1, 19.1.2, 19.1.3, 19.1.4, 19.1.5, 19.1.6, 19.1.7, 19.1.8, 19.1.9, 20.0, 20.0.1, 20.0.2, 20.0.3, 20.0.4, 20.0.5, 20.0.6, 20.0.7, 20.0.8, 20.0.8.5, 20.0.9, 20.0.10, 21.0.1, 21.0.2, 21.1, 21.1.1, 21.2, 21.2.1, 21.2.2, 21.2.3, 21.2.4, 22.1.0, 22.1.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 февраля 2021 г.
Дата обновления	9 февраля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/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/SB2021020971>