НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200318.8| 18 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в ПО компании Foxit Studio Photo

Идентификатор уязвимости	MITRE: CVE-2020-8878 CVE-2020-8880 CVE-2020-8881 CVE-2020-8882
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных CWE-787: Запись за границами буфера CWE-416: Использование после освобождения CWE-824: Обращение к неинициализированному указателю
Описание уязвимости	Эксплуатация уязвимостей позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных вредоносных страницы или файла. Уязвимость обусловлена некорректной обработкой файлов формата TIF и PSD.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Foxit Studio Photo до v3.6.6.918
Рекомендации по устранению	Обновить программное обеспечение.
Дата выявления	16 марта 2020 г.
Дата обновления	17 марта 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:N/UI:R/S:U/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)	Отсутствует (R)
Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Отсутствует (N)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Функциональная версия
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020031712 https://www.zerodayinitiative.com/advisories/ZDI-20-301/