НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210701.4 | 1 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Autodesk Design Review

Идентификатор уязвимости	MITRE: CVE-2021-27033 CVE-2021-27034 CVE-2021-27035 CVE-2021-27036 CVE-2021-27037 CVE-2021-27038 CVE-2021-27039
Идентификатор программной ошибки	CWE-415: Двойное освобождение CWE-122: Переполнение буфера в динамической памяти CWE-125: Чтение за пределами буфера CWE-787: Запись за границами буфера CWE-416: Использование после освобождения CWE-843: Доступ к ресурсам с использованием несовместимых типов (Смешение типов) CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных PNG, DF, DWF, PDF, PICT, TIFF файлов. Уязвимость обусловлена некорректной обработкой входных данных.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Autodesk Design Review: 2011, 2012, 2013, 2017, 2018, 2018 Hotfix 1, 2018 Hotfix 2
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	24 июня 2021 г.

Дата обновления	24 июня 2021 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/SB2021062401 https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0003