НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20210701.7 | 1 июля 2021 г.
Уровень опасности: ВЫСОКИЙ
Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Solid Edge SE2020

Идентификатор уязвимости	MITRE: CVE-2021-31342 CVE-2021-31342
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла формата DFT. Уязвимость обусловлена некорректной обработкой входных данных в библиотеке ugeom2d.dll.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Solid Edge SE2020: до 2020MP14 Solid Edge SE2021: до SE2021MP5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	10 июня 2021 г.
Дата обновления	10 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/SB2021061005 https://cert-portal.siemens.com/productcert/pdf/ssa-208356.pdf https://us-cert.cisa.gov/ics/advisories/icsa-21-159-09