

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20210610.2 | 10 июня 2021 г.
Уровень опасности: **ВЫСОКИЙ**
Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Visual Studio

Идентификатор уязвимости	MITRE: CVE-2021-27068
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в Visual Studio.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Visual Studio: 2019 v16.4, 2019 v16.7, 2019 v16.9
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 мая 2021 г.
Дата обновления	11 мая 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
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/SB2021051138>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27068>