

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211217.27 | 17 декабря 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Microsoft Remote Desktop Client

Идентификатор уязвимости	MITRE: CVE-2021-43233
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в клиенте удаленного рабочего стола.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows: 7, 8.1, 10, 10 20H2, 10 21H1, 10 21H2, 10 1507, 10 1511, 10 1607, 10 1703, 10 1709, 10 1803, 10 1809, 10 1903, 10 1909, 10 2004, 10 Gold, 10 Mobile, 10 S, 11 21H2, RT 8.1 Windows Server: до 2019 2004
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	14 декабря 2021 г.
Дата обновления	14 декабря 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Высокая (H)
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/SB2021121486>
<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43233>