

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220309.5 | 9 марта 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в Microsoft Remote Desktop Client

Идентификатор уязвимости	MITRE: CVE-2022-21990 CVE-2022-23285
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.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows: 7 - RT 8.1 Windows Server: 2008 - 2022
Рекомендации по устранению	Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.
Дата выявления	08 марта 2022 г.
Дата обновления	08 марта 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Требуется (R)

пользователем (UI)

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

Не определено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

Ссылки на источники

<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990>

<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285>

<https://www.cybersecurity-help.cz/vdb/SB2022030814>