НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220209.10 | 9 февраля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Microsoft Windows Runtime

Идентификатор уязвимости	MITRE: CVE-2022-21971
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: до 11 21H2 Windows Server: до 2022
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	8 февраля 2022 г.
Дата обновления	8 февраля 2022 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/SB2022020833 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21971