

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221228.16 | 28 декабря 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в Microsoft Raw Image Extension

Идентификатор уязвимости	MITRE: CVE-2022-44687
Идентификатор программной ошибки	CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Raw Image Extension: все версии
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	13 декабря 2022 г.
Дата обновления	13 декабря 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Требуется (R)
Масштаб последствий эксплуатации	Не изменяется (U)

уязвимости (S)

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

Не определено

Ссылки на источники

<http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-44687>