НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20201030.1 | 30 октября 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в библиотеке Microsoft Windows Codecs

Идентификатор уязвимости	MITRE: CVE-2020-17022
Идентификатор программной ошибки	CWE-119: Выполнение операций за пределами буфера памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла изображения. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке файла.
Категория уязвимого продукта	Операционные системы Microsoft и их компоненты
Уязвимый продукт	Windows 10 Version 1709 Windows 10 Version 1803 Windows 10 Version 1809 Windows 10 Version 1903 Windows 10 Version 1909 Windows 10 Version 2004
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	16 октября 2020 г.
Дата обновления	21 октября 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/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 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17022 https://nvd.nist.gov/vuln/detail/CVE-2020-17022