НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220405.8 | 5 апреля 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Apple iOS, iPadOS и Apple macOS Monterey

Идентификатор уязвимости	MITRE: CVE-2022-22675
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством запуска специально созданной вредоносной программы. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Операционные системы Apple и их компоненты
Уязвимый продукт	iPadOS: 15.0 19A346 - 15.4 19E241 Apple iOS: 15.0 19A346 - 15.4 19E241 macOS: 12.0 21A344 - 12.3 21E230
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	01 апреля 2022 г.
Дата обновления	01 апреля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Вектор атаки (AV)	Локальный (L)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий(L)
Необходимость взаимодействия с	Отсутствует (N)

пользователем (UI)	
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Высокая
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://support.apple.com/en-us/HT213219 http://support.apple.com/en-us/HT213220