НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210914.3 | 14 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Apple iOS

Идентификатор уязвимости	MITRE: CVE-2021-30860
Идентификатор программной ошибки	CWE-190: Целочисленное переполнение или циклический возврат
Описание уязвимости	Уязвимость позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF файла. Уязвимость обусловлена целочисленным переполнением буфера памяти в библиотеке визуализации изображений CoreGraphics.
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Apple iOS: 14.0 18A373, 14.0.1 18A393, 14.1 18A8395, 14.2 18B92, 14.2 18B111, 14.2.1 18B121, 14.3 18C66, 14.4 18D52, 14.4.1 18D61, 14.4.2 18D70, 14.5 18E199, 14.5.1 18E212, 14.6 18F72, 14.7 18G69, 14.7.1 18G82 iPadOS: 14.0 18A373, 14.0.1 18A393, 14.1 18A8395, 14.2 18B92, 14.2 18B111, 14.3 18C66, 14.4 18D52, 14.4.1 18D61, 14.4.2 18D70, 14.5 18E199, 14.5.1 18E212, 14.6 18F72, 14.7 18G69, 14.7 18G70, 14.7.1 18G82 WatchOS: 7.0 18R382, 7.0.1 18R395, 7.0.2 18R402, 7.0.3 18R410, 7.1 18R590, 7.2 18S564, 7.3 18S801, 7.3.1 18S811, 7.3.2 18S821, 7.3.3 18S830, 7.4 18T195, 7.4.1 18T201, 7.5 18T567, 7.6 18U63, 7.6.1 18U70 MacOS: 10.15 19A583, 10.15 19A602, 10.15 19A603, 10.15.1 19B88, 10.15.2 19C57, 10.15.3 19D76, 10.15.4 19E266, 10.15.4 19E287, 10.15.5 19F96, 10.15.5 19F101, 10.15.6 19G73, 10.15.6 19G2021, 10.15.7 19H2, 10.15.7 19H4, 10.15.7 19H15, 10.15.7 19H114, 10.15.7 19H512, 10.15.7 19H524, 10.15.7 19H1030, 10.15.7 19H1217,

	10.15.7 19H1323
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	25 августа 2021 г.
Дата обновления	13 сентября 2021 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	Высокая
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021091321 https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/ https://support.apple.com/en-us/HT212807 https://support.apple.com/en-us/HT212805