НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210927.2 | 27 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости Apple iOS

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
Дата выявления	25 августа 2021 г.
Дата обновления	13 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-30860	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных вредоносных файлов PDF. Уязвимость обусловлена целочисленным переполнением в компоненте CoreGraphics. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат	8.8

	Рекомендации по устранению: обновить программное обеспечение	
MITRE: CVE-2021-30858	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения при обработке HTML-содержимого в WebKit. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-30869	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код с привилегиями суперпользователя целевой системы посредством запуска специально созданного вредоносного приложения. Уязвимость обусловлена ошибкой смешения типов в ядре ОС XNU. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов) Рекомендации по устранению: обновить программное обеспечение	8.8

Ссылки на источники	https://support.apple.com/en-us/HT212807 https://www.cybersecurity-help.cz/vdb/SB2021092317 https://support.apple.com/en-us/HT212825 https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/