

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20211217.2 | 17 декабря 2021 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Apple Safari

Категория уязвимого продукта	Операционные системы Apple и их компоненты
Уязвимый продукт	Apple Safari: до 15.1
Дата выявления	15 декабря 2021 г.
Дата обновления	15 декабря 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-30934	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8

<p>MITRE: CVE-2021-30936 CVE-2021-30951</p>	<p>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.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-416: Использование после освобождения</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-30952</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена целочисленным переполнением.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-190: Целочисленное переполнение или циклический возврат</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-30984</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена состоянием гонки.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-362: Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>
<p>MITRE: CVE-2021-30953</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-125: Чтение за пределами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	<p>8.8</p>

MITRE: CVE-2021-30954	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов)</p> <p>Рекомендации по устранению: обновить программное обеспечение</p>	8.8
--------------------------	---	-----

Ссылки на источники	<p>https://www.cybersecurity-help.cz/vdb/SB2021121510</p> <p>http://support.apple.com/en-us/HT212978</p>
---------------------	---