

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220127.7 | 27 января 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Apple iOS

| | |
|------------------------------|---|
| Категория уязвимого продукта | Операционные системы Apple и их компоненты |
| Уязвимый продукт | Apple iOS: до 15.2.1 19C63 iPadOS: до 15.2.1 19C63 |
| Дата выявления | 26 января 2022 г. |
| Дата обновления | 26 января 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|--------------------------|--|----------------------|
| MITRE: CVE-2022-22584 | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. 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-2022-22578</p> | <p>Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-264: Уязвимость в управлении доступом, привилегиями и разрешениями</p> <p>Рекомендации по устранению: обновить программное обеспечение</p> | <p>8.8</p> |
| <p>MITRE: CVE-2022-22587</p> | <p>Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>Рекомендации по устранению: обновить программное обеспечение</p> | <p>8.8</p> |
| <p>MITRE: CVE-2022-22593</p> | <p>Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/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> | <p>8.8</p> |
| <p>MITRE: CVE-2022-22579</p> | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного STL-файла. Уязвимость обусловлена граничным условием.</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-2022-22590 | <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> | 8.8 |
|--------------------------|--|-----|

| | |
|---------------------|--|
| Ссылки на источники | <p>https://www.cybersecurity-help.cz/vdb/SB2022012633</p> <p>http://support.apple.com/en-us/HT213056</p> <p>http://support.apple.com/en-us/HT213053</p> |
|---------------------|--|