# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200429.1 | 29 апреля 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

## Выполнение произвольного кода в FFmpeg

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-12284 |
| Идентификатор программной ошибки | CWE-122: Переполнение буфера в динамической памяти |
| Описание уязвимости | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством передачи специально сформированных вредоносных данных. Уязвимость обусловлена переполнением буфера при обработке параметра JPEG_MARKER_SOS в файле libavcodec/cbs_jpeg.c. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимое ПО | FFmpeg до v4.2.2 включительно |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 28 апреля 2020 г. |
| Дата обновления | 28 апреля 2020 г. |
| Оценка критичности уязвимости (CVSSv3.0) | 9.8 AV:N/AC:L/PR:N/UI:N/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) | Отсутствует (N) |
| 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 | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Отсутствует |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | https://nvd.nist.gov/vuln/detail/CVE-2020-12284<br>https://www.cybersecurity-help.cz/vdb/SB2020042816 |