# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200318.4 | 18 марта 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

## Множественные уязвимости в Adobe Reader и Acrobat

| | |
|---|---|
| Идентификатор уязвимости | MITRE: CVE-2020-3792<br>CVE-2020-3793<br>CVE-2020-3795<br>CVE-2020-3797<br>CVE-2020-3799<br>CVE-2020-3801<br>CVE-2020-3802<br>CVE-2020-3805<br>CVE-2020-3807 |
| Идентификатор программной ошибки | CWE-787: Запись за границами буфера<br>CWE-121: Переполнение буфера в стеке<br>CWE-416: Использование после освобождения<br>CWE-120: Копирование содержимого буфера без проверки размера входных данных<br>CWE-119: Выполнение операций за пределами буфера памяти |
| Описание уязвимости | Эксплуатация уязвимостей позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного файла формата PDF. Уязвимости обусловлены некорректной работой с памятью при обработке файлов формата PDF. |
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимое ПО | Acrobat DC для Windows и macOS версии 2020.006.20034 и ниже<br>Acrobat 2017 для Windows версии 2017.011.30158 и ниже<br>Acrobat Reader 2017 для macOS версии 2017.011.30158 и ниже |

| | |
|---|---|
| | Acrobat 2015 для Windows и macOS версии 2015.006.30510 и ниже<br>Acrobat Reader 2015 для Windows и macOS версии 2015.006.30510 и ниже |
| Рекомендации по устранению | Обновить программное обеспечение. |
| Дата выявления | 13 декабря 2019 г. |
| Дата обновления | 12 марта 2020 г. |
| Оценка критичности уязвимости (CVSSv3.1) | 7.7 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 | Наличие не подтверждено |
| Наличие средств устранения уязвимости | Официальное решение |
| Достоверность сведений об уязвимости | Сведения подтверждены |
| Ссылки на источники | https://www.cybersecurity-help.cz/vdb/SB2020031714 |