

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230111.11 | 11 января 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в Adobe InDesign

|                              |                                    |
|------------------------------|------------------------------------|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт             | Adobe InDesign: 17.0 - 17.4        |
| Дата выявления               | 10 января 2023 г.                  |
| Дата обновления              | 10 января 2023 г.                  |

| Идентификатор уязвимости | Описание уязвимости                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Базовый уровень CVSS |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| MITRE:<br>CVE-2023-21587 | <p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-122: Переполнение буфера в динамической памяти</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> | 7.8                  |

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |            |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <p>MITRE:<br/>CVE-2023-21588</p>                    | <p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-20: Некорректная проверка входных данных</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p> | <p>7.8</p> |
| <p>MITRE:<br/>CVE-2023-21589<br/>CVE-2023-21590</p> | <p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</p> <p>CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.</p>                          | <p>7.8</p> |

Ссылки на  
источники

<http://helpx.adobe.com/security/products/indesign/apsb23-07.html>