НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230111.12 | 11 января 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Adobe InCopy

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	InCopy: 18.0, 17.0 - 17.4
Дата выявления	10 января 2023 г.
Дата обновления	10 января 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-21594	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-122: Переполнение буфера в динамической памяти 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.	7.8

MITRE: CVE-2023-21595 CVE-2023-21597	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-787: Запись за границами буфера 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.	7.8
MITRE: CVE-2023-21596	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CWE-20: Некорректная проверка входных данных 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.	7.8

Ссылки на источники	http://helpx.adobe.com/security/products/incopy/apsb23-08.html