

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20230315.3 | 15 марта 2023 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Adobe Illustrator

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Illustrator: 26.0 - 26.5.2, 25.0 - 25.4.8, 24.0 - 24.3.2, 23.0 - 23.1, 22.0 - 22.1
Дата выявления	14 марта 2023 г.
Дата обновления	14 марта 2023 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2023-25859	<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>	7.8

<p>MITRE: CVE-2023-25860 CVE-2023-25861</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:H/I:H/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>
<p>MITRE: CVE-2023-26426</p>	<p>Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой использования после освобождения.</p> <p>CVSSv3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</p> <p>CWE-416: Использование после освобождения</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>Ссылки на источники http://helpx.adobe.com/security/products/illustrator/apsb23-19.html</p>		