

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220516.20 | 16 мая 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в Adobe Framemaker

| | |
|------------------------------|-------------------------------------|
| Категория уязвимого продукта | Прикладное программное обеспечение |
| Уязвимый продукт | Adobe Framemaker: 2019.0 - 2020.0.4 |
| Дата выявления | 11 мая 2022 г. |
| Дата обновления | 11 мая 2022 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|--|--|----------------------|
| MITRE: CVE-2022-28821 CVE-2022-28822 CVE-2022-28825 CVE-2022-28826 CVE-2022-28827 CVE-2022-28828 CVE-2022-28829 CVE-2022-28830 | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</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> | 8.8 |

| | | |
|--|---|-----|
| MITRE: CVE-2022-28823 CVE-2022-28824 | <p>Эксплуатация уязвимости позволяет удаленному 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:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</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> | 8.8 |
| Ссылки на источники | http://helpx.adobe.com/security/products/framesmaker/apsb22-27.html | |