НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210705.5 | 5 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в OpenEXR

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	OpenEXR: 3.0.0 beta, 3.0.1, 3.0.2, 3.0.3, 3.0.4
Дата выявления	27 июня 2021 г.
Дата обновления	27 июня 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-3598	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством передачи в приложение специально сформированных вредоносных данных. Уязвимость обусловлена некорректным определением границ памяти в функции readChars () файла ImfIO.h. CVSSv3.1: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	8.1

MITRE: CVE-2021-3605	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством передачи в приложение специально сформированных вредоносных данных. Уязвимость обусловлена некорректным определением границ памяти в функции rleUncompress файла ImfRle.cpp. CVSSv3.1: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	8.1

Ссылки на источники	https://github.com/AcademySoftwareFoundation/openexr/pull/1036 https://www.cybersecurity-help.cz/vdb/SB2021062707