НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210514.6 | 14 мая 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Adobe Reader и Acrobat

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Acrobat DC v2021.001.20150 и более ранние версии Adobe Acrobat v2020.001.30020 и более ранние версии Adobe Acrobat Reader DC v2021.001.20150 и более ранние версии Adobe Acrobat Reader v2020.001.30020 и более ранние версии
Дата выявления	11 мая 2021 г.
Дата обновления	11 мая 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-28550	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректным обнулением указателей на ячейки памяти. CVSSv3.1: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	8.8

MITRE: CVE-2021-28562 CVE-2021-28553	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректным обнулением указателей на ячейки памяти. CVSSv3.1: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	
MITRE: CVE-2021-28561 CVE-2021-28560 CVE-2021-28558 CVE-2021-28557 CVE-2021-28565 CVE-2021-28564	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректным определением границ буфера памяти. CVSSv3.1: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти CWE-122: Переполнение буфера в динамической памяти CWE-125: Чтение за пределами буфера CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021051143 https://helpx.adobe.com/security/products/acrobat/apsb21-29.html