НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220112.10 | 12 января 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Adobe Acrobat

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Acrobat: до 2017.011.30204 Adobe Acrobat Reader: до 2017.011.30204 Adobe Acrobat DC: до 2021.007.20099 Adobe Acrobat Reader DC: до 2021.007.20099
Дата выявления	11 января 2022 г.
Дата обновления	11 января 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-44707 CVE-2021-45061 CVE-2021-45068	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2021-44701 CVE-2021-44704 CVE-2021-44706 CVE-2021-44710 CVE-2021-45062 CVE-2021-45064	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой использования после освобождения. CVSSv3.0: 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	8.8
MITRE: CVE-2021-45060	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена некорректной проверкой входных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-44711	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена целочисленным переполнением. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-44708 CVE-2021-44709	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение	8.8

MITRE: CVE-2021-44705	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена некорректной обработкой PDF-файлов. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-824: Обращение к неинициализированному указателю Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-44703	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: обновить программное обеспечение	8.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022011133 http://helpx.adobe.com/security/products/acrobat/apsb22-01.html