НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200513.13 | 13 мая 2020 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Adobe Acrobat и Reader

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Adobe Acrobat DC до v2020.006.20042 Adobe Acrobat Reader DC до v2020.006.20042 Adobe Acrobat до v2017.011.30166 Adobe Reader до v2017.011.30166
Дата выявления	12 мая 2020 г.
Дата обновления	12 мая 2020 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2020-9606 CVE-2020-9607	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена отсутствием обнуления указателей на освобожденные ячейки буфера памяти при обработке объектов Field. 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-2020-9604 CVE-2020-9605	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена некорректным определением границ буфера памяти на основе кучи. 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-119: Выполнение операций за пределами буфера памяти Рекомендации по устранению: обновить программное обеспечение.	8.8
MITRE: CVE-2020-9612	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке изображений JPEG2000. 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-2020-9614 CVE-2020-9613 CVE-2020-9596 CVE-2020-9592	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена обходом функций безопасности уязвимого приложения. 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-264: Уязвимость в управлении доступом, привилегиями и разрешениями Рекомендации по устранению: обновить программное обеспечение.	8.8

MITRE: CVE-2020-9594 CVE-2020-9597	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена возможностью записи данных за пределами буфера 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-2020-9615	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена наличием состояния гонки при обработке 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-362: Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (Состояние гонки) Рекомендации по устранению: обновить программное обеспечение.	8.8

Ссылки на источники	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html https://www.cybersecurity-help.cz/vdb/SB2020051221