НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20210917.23 | 17 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Adobe

Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Adobe Acrobat DC: 2020.001.30020, 2020.001.30025, 2020.004.30005, 2020.004.30006, 2020.006.20034, 2020.006.20042, 2020.009.20063, 2020.009.20074, 2020.012.20041, 2020.012.20048, 2020.013.20064, 2020.013.20066, 2020.013.20074, 2021.001.20135, 2021.001.20149, 2021.001.20150, 2021.001.20155, 2021.005.20054, 2021.005.20058, 2021.005.20060, 2021.005.20148 Adobe Acrobat: 2017.008.30051, 2017.011.30066, 2017.011.30068, 2017.011.30070, 2017.011.30078, 2017.011.30096, 2017.011.30102, 2017.011.30105, 2017.011.30120, 2017.011.30127, 2017.011.30148, 2017.011.30150, 2017.011.30152, 2017.011.30156, 2017.011.30158, 2017.011.30166, 2017.011.30171, 2017.011.30175, 2017.011.30180, 2017.011.30188, 2017.011.30190, 2017.011.30194, 2017.011.30196, 2017.011.30197, 2017.011.30199 Adobe Acrobat Reader DC: 2020.001.30020, 2020.001.30025, 2020.004.30005, 2020.004.30006, 2020.006.20034, 2020.006.20042, 2020.009.20063, 2020.009.20074, 2020.012.20041, 2020.012.20048, 2020.013.20064, 2020.013.20066, 2020.013.20074, 2021.001.20135, 2021.001.20149, 2021.001.20150, 2021.001.20155, 2021.005.20054, 2021.005.20058, 2021.005.20060, 2021.005.20148 Adobe Reader: 2017.008.30051, 2017.011.30066, 2017.011.30068, 2017.011.30070, 2017.011.30078, 2017.011.30099, 2017.011.30102, 2017.011.30105, 2017.011.30152, 2017.011.30156, 2017.011.30158, 2017.011.30166, 2017.011.30171, 2017.011.30175, 2017.011.30199

Дата выявления	14 сентября 2021 г.
Дата обновления	14 сентября 2021 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-39841	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена ошибкой смешения типов. 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-843: Доступ к ресурсам с использованием несовместимых типов (смешение типов) Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-39842 CVE-2021-39836 CVE-2021-39837 CVE-2021-39838 CVE-2021-39839 CVE-2021-39840 CVE-2021-39859	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного 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-2021-39863	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного 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-2021-35982	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена некорректной загрузкой DLL-библиотек. 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-427: Неконтролируемый элемент пути поиска Рекомендации по устранению: обновить программное обеспечение	8.8
MITRE: CVE-2021-39845 CVE-2021-39846	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного 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
MITRE: CVE-2021-39843	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного 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

Ссылки на источники	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html https://www.cybersecurity-help.cz/vdb/SB2021091436