НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-11-17.1 | 17 ноября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-26347	Adobe ColdFusion	Сетевой	OSI	2023-11-15	✓
2	Высокая	CVE-2023-44351	Adobe ColdFusion	Сетевой	ACE	2023-11-15	✓
3	Критическая	CVE-2023-44350	Adobe ColdFusion	Сетевой	ACE	2023-11-15	✓
4	Высокая	CVE-2023-36041	Microsoft Excel	Локальный	ACE	2023-11-15	✓
5	Высокая	CVE-2023-36037	Microsoft Excel	Локальный	PE	2023-11-15	✓
6	Высокая	CVE-2023-47073	Adobe After Effects	Локальный	ACE	2023-11-15	✓
7	Высокая	CVE-2023-47070	Adobe After Effects	Локальный	ACE	2023-11-15	✓
8	Высокая	CVE-2023-47069	Adobe After Effects	Локальный	ACE	2023-11-15	✓
9	Высокая	CVE-2023-47068	Adobe After Effects	Локальный	ACE	2023-11-15	✓
10	Высокая	CVE-2023-47067	Adobe After Effects	Локальный	ACE	2023-11-15	✓
11	Высокая	CVE-2023-47066	Adobe After Effects	Локальный	ACE	2023-11-15	✓
12	Высокая	CVE-2023-38151	Microsoft Host Integration Server	Сетевой	ACE	2023-11-14	✓
13	Высокая	CVE-2023-44337	Adobe Acrobat и Adobe Reader	Локальный	ACE	2023-11-14	✓

14	Высокая	CVE-2023-44338	Adobe Acrobat и Adobe Reader	Локальный	ACE	2023-11-14	✓
15	Высокая	CVE-2023-44359	Adobe Acrobat и Adobe Reader	Локальный	ACE	2023-11-14	✓
16	Высокая	CVE-2023-44365	Adobe Reader и Adobe Acrobat	Локальный	ACE	2023-11-14	✓
17	Высокая	CVE-2023-44366	Adobe Reader и Adobe Acrobat	Локальный	ACE	2023-11-14	✓
18	Высокая	CVE-2023-44367	Adobe Acrobat и Adobe Reader	Локальный	ACE	2023-11-14	✓
19	Высокая	CVE-2023-44371	Adobe Acrobat и Adobe Reader	Локальный	ACE	2023-11-14	✓
20	Высокая	CVE-2023-44336	Adobe Acrobat и Adobe Reader	Сетевой	ACE	2023-11-14	✓
21	Высокая	CVE-2023-44372	Adobe Acrobat и Adobe Reader	Сетевой	ACE	2023-11-14	✓
22	Высокая	CVE-2023-36017	Microsoft Windows Scripting Engine	Сетевой	ACE	2023-11-14	✓
23	Критическая	CVE-2023-34060	VMware Cloud Director	Сетевой	OSI	2023-11-14	✓
24	Критическая	CVE-2023-6112	Google Chrome	Сетевой	ACE	2023-11-14	✓
25	Критическая	CVE-2023-5997	Google Chrome	Сетевой	ACE	2023-11-14	✓
26	Высокая	CVE-2023-36396	Microsoft Windows Compressed Folder	Локальный	ACE	2023-11-14	✓
27	Высокая	CVE-2023-36045	Microsoft Office Graphics	Локальный	ACE	2023-11-14	✓
28	Критическая	CVE-2023-36028	Microsoft Protected Extensible Authentication Protocol (PEAP)	Сетевой	ACE	2023-11-14	✓

29	Высокая	CVE-2023-36393	Microsoft Windows User Interface Application Core	Локальный	ACE	2023-11-14	✓
30	Высокая	CVE-2023-36033	Microsoft Windows DWM Core Library	Локальный	ACE	2023-11-14	✓
31	Высокая	CVE-2023-36025	Microsoft Windows SmartScreen	Сетевой	OSI	2023-11-14	✓
32	Высокая	CVE-2023-36036	Microsoft Windows Cloud Files Mini Filter Driver	Локальный	ACE	2023-11-14	✓
33	Критическая	CVE-2023-46853	memcached	Сетевой	ACE	2023-11-13	✓
34	Высокая	CVE-2023-46852	memcached	Сетевой	ACE	2023-11-13	✓
35	Высокая	CVE-2023-5941	FreeBSD	Локальный	ACE	2023-11-10	✓

1

Краткое описание: Получение конфиденциальной информации в Adobe ColdFusion

Идентификатор уязвимости: CVE-2023-26347

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Adobe ColdFusion: 2021 - 2023 Update 5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb23-52.html

2

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2023-44351

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Adobe ColdFusion: 2021 - 2023 Update 5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb23-52.html

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2023-44350

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Adobe ColdFusion: 2021 - 2023 Update 5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

3 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/coldfusion/apsb23-52.html

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2023-36041

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Excel: 2016
Microsoft Office: 2019
Microsoft Office LTSC 2021: 32 bit editions - 2021 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

4 **Последствия эксплуатации:** выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36041

Краткое описание: Повышение привилегий в Microsoft Excel

Идентификатор уязвимости: CVE-2023-36037

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Excel: 2016
Microsoft Office: 2019
Microsoft Office LTSC 2021: 32 bit editions - 2021 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

5 **Последствия эксплуатации:** повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36037

6

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-47073

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: до 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-66.html

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-47070

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: до 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

7 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-66.html

8

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-47069

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: до 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-66.html

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-47068

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: до 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

9 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-66.html

10

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-47067

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: до 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-66.html

11

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-47066

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe After Effects: до 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-15 / 2023-11-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-66.html

Краткое описание: Выполнение произвольного кода в Microsoft Host Integration Server

Идентификатор уязвимости: CVE-2023-38151

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Host Integration Server: 2020
OLE DB Provider for DB2 V7: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

12

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38151

13

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44337

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 23.006.20360

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

14

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44338

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 23.006.20360

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

15

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44359

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Acrobat: 15.006.30306 - 23.006.20360
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

16

Краткое описание: Выполнение произвольного кода в Adobe Reader и Adobe Acrobat

Идентификатор уязвимости: CVE-2023-44365

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 23.006.20360

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

17

Краткое описание: Выполнение произвольного кода в Adobe Reader и Adobe Acrobat

Идентификатор уязвимости: CVE-2023-44366

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 23.006.20360

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

18

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44367

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Acrobat: 15.006.30306 - 23.006.20360
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

19

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44371

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Acrobat: 15.006.30306 - 23.006.20360
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

20

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44336

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Acrobat: 15.006.30306 - 23.006.20360
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

21

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Adobe Reader

Идентификатор уязвимости: CVE-2023-44372

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat и Adobe Reader:
Adobe Acrobat: 15.006.30306 - 23.006.20360
Adobe Reader: 20.005.30331 - 2020.013.20074

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb23-54.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Scripting Engine

Идентификатор уязвимости: CVE-2023-36017

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Microsoft Windows Scripting Engine:
Windows: 10 - 11 23H2
Windows Server: 2008 R2 - 2022 23H2
Microsoft Internet Explorer: 11 - 11.1790.17763.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

22 **Последствия эксплуатации:** выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36017

Краткое описание: Получение конфиденциальной информации в VMware Cloud Director

Идентификатор уязвимости: CVE-2023-34060

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: VMware Cloud Director: 10.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: получение конфиденциальной информации

23 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0026.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-6112

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.124

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: выполнение произвольного кода

24 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_14.html
- http://crbug.com/1499298

25

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-5997

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 119.0.6045.124

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_14.html
- http://crbug.com/1497997

Краткое описание: Выполнение произвольного кода в Microsoft Windows Compressed Folder

Идентификатор уязвимости: CVE-2023-36396

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows Compressed Folder:
Windows: 10 - 11 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

26

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36396

Краткое описание: Выполнение произвольного кода в Microsoft Office Graphics

Идентификатор уязвимости: CVE-2023-36045

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Office Graphics:
Microsoft Office LTSC 2021: 32 bit editions - 2021 for Mac
Microsoft Office: 2019
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

27 **Последствия эксплуатации:** выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36045

28

Краткое описание: Выполнение произвольного кода в Microsoft Protected Extensible Authentication Protocol (PEAP)

Идентификатор уязвимости: CVE-2023-36028

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Protected Extensible Authentication Protocol (PEAP):
Windows: 10 - 11 23H2
Windows Server: 2016 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36028

29

Краткое описание: Выполнение произвольного кода в Microsoft Windows User Interface Application Core

Идентификатор уязвимости: CVE-2023-36393

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Windows User Interface Application Core:
Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36393

30

Краткое описание: Выполнение произвольного кода в Microsoft Windows DWM Core Library

Идентификатор уязвимости: CVE-2023-36033

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Microsoft Windows DWM Core Library:
Windows: 10 - 11 23H2
Windows Server: 2019 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36033

31

Краткое описание: Получение конфиденциальной информации в Microsoft Windows SmartScreen

Идентификатор уязвимости: CVE-2023-36025

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Windows SmartScreen:
Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36025

32

Краткое описание: Выполнение произвольного кода в Microsoft Windows Cloud Files Mini Filter Driver

Идентификатор уязвимости: CVE-2023-36036

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Microsoft Windows Cloud Files Mini Filter Driver:
Windows: 10 - 11 23H2
Windows Server: 2008 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-14 / 2023-11-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36036

33

Краткое описание: Выполнение произвольного кода в memcached

Идентификатор уязвимости: CVE-2023-46853

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: memcached: 1.0.0 - 1.6.21

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-13 / 2023-11-13

Ссылки на источник:

- http://github.com/memcached/memcached/compare/1.6.21...1.6.22
- http://github.com/memcached/memcached/commit/6987918e9a3094ec4fc8976f01f769f624d790fa

34

Краткое описание: Выполнение произвольного кода в memcached

Идентификатор уязвимости: CVE-2023-46852

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: memcached: 1.0.0 - 1.6.21

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-13 / 2023-11-13

Ссылки на источник:

- http://github.com/memcached/memcached/commit/76a6c363c18cfe7b6a1524ae64202ac9db330767
- http://github.com/memcached/memcached/compare/1.6.21...1.6.22

Краткое описание: Выполнение произвольного кода в FreeBSD

Идентификатор уязвимости: CVE-2023-5941

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: FreeBSD: 12.4 - 14.0

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

35 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-11-10 / 2023-11-10

Ссылки на источник:

- http://security.freebsd.org/advisories/FreeBSD-SA-23:15.stdio.asc