НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-12-13.1 | 13 декабря 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-36006	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2023-12-12	✓
2	Высокая	CVE-2023-35639	Microsoft ODBC Driver	Сетевой	ACE	2023-12-12	✓
3	Высокая	CVE-2023-48634	Adobe After Effects	Локальный	ACE	2023-12-12	✓
4	Высокая	CVE-2023-48633	Adobe After Effects	Локальный	ACE	2023-12-12	✓
5	Высокая	CVE-2023-48632	Adobe After Effects	Локальный	ACE	2023-12-12	✓
6	Высокая	CVE-2023-47063	Adobe Illustrator	Локальный	ACE	2023-12-12	✓
7	Высокая	CVE-2023-47075	Adobe Illustrator	Локальный	ACE	2023-12-12	✓
8	Высокая	CVE-2023-47074	Adobe Illustrator	Локальный	ACE	2023-12-12	✓
9	Высокая	CVE-2023-21740	Microsoft Windows Media	Локальный	ACE	2023-12-12	✓
10	Высокая	CVE-2023-48630	Adobe Substance 3D Sampler	Локальный	ACE	2023-12-12	✓
11	Высокая	CVE-2023-48629	Adobe Substance 3D Sampler	Локальный	ACE	2023-12-12	✓
12	Высокая	CVE-2023-48628	Adobe Substance 3D Sampler	Локальный	ACE	2023-12-12	✓
13	Высокая	CVE-2023-48627	Adobe Substance 3D Sampler	Локальный	ACE	2023-12-12	✓

14	Высокая	CVE-2023-48626	Adobe Substance 3D Sampler	Локальный	ACE	2023-12-12	✓
15	Высокая	CVE-2023-48625	Adobe Substance 3D Sampler	Локальный	ACE	2023-12-12	✓
16	Высокая	CVE-2023-48639	Adobe Substance 3D Designer	Локальный	ACE	2023-12-12	✓
17	Критическая	CVE-2023-36019	Microsoft Power Platform Connector	Сетевой	XSS\CSS	2023-12-12	✓
18	Высокая	CVE-2023-35628	Microsoft Windows MSHTML Platform	Сетевой	ACE	2023-12-12	✓
19	Критическая	CVE-2023-6448	Unitronics Vision Series PLCs and HMIs	Сетевой	OSI	2023-12-12	✓
20	Высокая	CVE-2023-6186	LibreOffice	Смежная сеть	OSI	2023-12-12	✓
21	Высокая	CVE-2023-6185	LibreOffice	Смежная сеть	ACE	2023-12-12	✓
22	Высокая	CVE-2023-5996	Chrome OS	Сетевой	ACE	2023-12-11	✓
23	Высокая	CVE-2023-6347	Chrome OS	Сетевой	ACE	2023-12-11	✓
24	Высокая	CVE-2023-5997	Chrome OS	Сетевой	ACE	2023-12-11	✓
25	Критическая	CVE-2023-6345	Chrome OS	Сетевой	ACE	2023-12-11	✓
26	Высокая	CVE-2023-42894	macOS Sonoma, Ventura, Monterey	Сетевой	OSI	2023-12-11	✓
27	Высокая	CVE-2023-42924	macOS Sonoma, Ventura	Сетевой	OSI	2023-12-11	✓
28	Высокая	CVE-2023-42884	macOS Sonoma, Ventura, Monterey	Сетевой	OSI	2023-12-11	✓

29	Критическая	CVE-2023-42886	macOS Sonoma, Ventura, Monterey	Сетевой	ACE	2023-12-11	✓
30	Высокая	CVE-2023-42922	macOS Sonoma, Ventura, Monterey	Сетевой	OSI	2023-12-11	✓
31	Критическая	CVE-2023-42899	macOS Sonoma, Ventura, Monterey	Сетевой	ACE	2023-12-11	✓
32	Критическая	CVE-2023-42891	macOS Sonoma, Ventura, Monterey	Сетевой	OSI	2023-12-11	✓
33	Высокая	CVE-2023-42919	macOS Sonoma, Ventura, Monterey	Сетевой	OSI	2023-12-11	✓
34	Критическая	CVE-2023-42914	macOS Sonoma, Ventura, Monterey	Сетевой	SB	2023-12-11	✓
35	Высокая	CVE-2023-42932	macOS Sonoma, Ventura, Monterey	Сетевой	RLF	2023-12-11	✓
36	Высокая	CVE-2023-42890	WebKitGTK+ и WPE WebKit	Сетевой	ACE	2023-12-11	✗
37	Не определено	None	WordPress	Не определено	ACE	2023-12-08	✓

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-36006

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: 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

1 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36006

2

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-35639

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: 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: 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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35639

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-48634

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe After Effects: 1.0 - 24.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-75.html

4

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-48633

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe After Effects: 1.0 - 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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-75.html

5

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2023-48632

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: 1.0 - 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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb23-75.html

6

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2023-47063

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.0

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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb23-68.html

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2023-47075

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.0

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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb23-68.html

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2023-47074

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Illustrator: 22.0 - 28.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

8 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb23-68.html

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-21740

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 23H2
Windows Server: 2008 R2 - 2022 23H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21740

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Sampler

Идентификатор уязвимости: CVE-2023-48630

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler: 0.5.0 - 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

10 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Sampler

Идентификатор уязвимости: CVE-2023-48629

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler: 0.5.0 - 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

11 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Sampler

Идентификатор уязвимости: CVE-2023-48628

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler: 0.5.0 - 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Sampler

Идентификатор уязвимости: CVE-2023-48627

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler: 0.5.0 - 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

13 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Sampler

Идентификатор уязвимости: CVE-2023-48626

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler: 0.5.0 - 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

14 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Sampler

Идентификатор уязвимости: CVE-2023-48625

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler: 0.5.0 - 4.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

15 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d-sampler/apsb23-74.html

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Designer

Идентификатор уязвимости: CVE-2023-48639

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: 5.0.0 - 13.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

16 **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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_designer/apsb23-76.html

Краткое описание: Межсайтовый скриптинг в Microsoft Power Platform

Идентификатор уязвимости: CVE-2023-36019

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Microsoft Power Platform: все версии
Azure Logic Apps: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: межсайтовый скриптинг

17 **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: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36019

18

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-35628

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: 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: 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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-35628

19

Краткое описание: Получение конфиденциальной информации в Unitronics Vision

Идентификатор уязвимости: CVE-2023-6448

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Unitronics Vision: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

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: 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: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems
- http://www.waterisac.org/portal/tlpclear-cisa-releases-alert-exploitation-unitronics-plcs-used-water-and-wastewater-systems
- http://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal
- https://bdu.fstec.ru/vul/2023-08540

Краткое описание: Получение конфиденциальной информации в LibreOffice

Идентификатор уязвимости: CVE-2023-6186

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: LibreOffice: 7.0.0.1 - 7.6.3.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

20 **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: 8.3 AV:A/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://www.libreoffice.org/about-us/security/advisories/cve-2023-6186

21

Краткое описание: Выполнение произвольного кода в LibreOffice

Идентификатор уязвимости: CVE-2023-6185

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: LibreOffice: 7.0.0.1 - 7.6.2.1

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: 8.3 AV:A/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-12 / 2023-12-12

Ссылки на источник:

- http://www.libreoffice.org/about-us/security/advisories/cve-2023-6185

22

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-5996

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.343

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

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: 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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/12/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-07841

23

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-6347

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.343

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

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: 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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/12/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-08361

24

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-5997

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.343

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

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: 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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/12/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-08092

25

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-6345

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: Chrome OS: до 114.0.5735.343

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

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: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-12-11 / 2023-12-11

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/12/long-term-support-channel-update-for.html
- https://bdu.fstec.ru/vul/2023-08264

Краткое описание: Получение конфиденциальной информации в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42894

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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: 7.5 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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Получение конфиденциальной информации в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42924

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

27 **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:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214038

Краткое описание: Получение конфиденциальной информации в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42884

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

28 **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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Выполнение произвольного кода в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42886

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: выполнение произвольного кода

29 **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:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Получение конфиденциальной информации в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42922

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

30 **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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Выполнение произвольного кода в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42899

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

31 **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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Получение конфиденциальной информации в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42891

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

32 **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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Получение конфиденциальной информации в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42919

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

33 **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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Обход безопасности в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42914

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

34 **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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

Краткое описание: Чтение локальных файлов в macOS Sonoma

Идентификатор уязвимости: CVE-2023-42932

Идентификатор программной ошибки: Не определено

Уязвимый продукт: macOS Sonoma: до 14.2
macOS Ventura: до 13.6.3
macOS Monterey: до 12.7.2

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

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: чтение локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-12-11 / 2023-12-11

Ссылки на источник:

- https://support.apple.com/en-us/HT214036
- https://support.apple.com/en-us/HT214037
- https://support.apple.com/en-us/HT214038

36

Краткое описание: Выполнение произвольного кода в WebKitGTK+

Идентификатор уязвимости: CVE-2023-42890

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

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

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: 2023-12-11 / 2023-12-11

Ссылки на источник:

- http://support.apple.com/en-us/HT214036

Краткое описание: Выполнение произвольного кода в WordPress

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: WordPress: 6.4 - 6.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

37 **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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2023-12-08 / 2023-12-08

Ссылки на источник:

- http://wordpress.org/documentation/wordpress-version/version-6-4-2/