

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-11-15.1 | 15 ноября 2024 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-49027	Microsoft	Локальный	ACE	2024-11-12	✓
2	Высокая	CVE-2024-49026	Microsoft	Локальный	ACE	2024-11-12	✓
3	Высокая	CVE-2024-49028	Microsoft	Локальный	OSI	2024-11-12	✓
4	Высокая	CVE-2024-49030	Microsoft	Локальный	ACE	2024-11-12	✓
5	Высокая	CVE-2024-49029	Microsoft	Локальный	ACE	2024-11-12	✓
6	Высокая	CVE-2024-49514	Adobe Photoshop	Локальный	ACE	2024-11-12	✓
7	Высокая	CVE-2024-49519	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
8	Высокая	CVE-2024-47426	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
9	Высокая	CVE-2024-47427	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
10	Высокая	CVE-2024-47428	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
11	Высокая	CVE-2024-47429	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
12	Высокая	CVE-2024-47430	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
13	Высокая	CVE-2024-49515	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓

14	Высокая	CVE-2024-49516	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
15	Высокая	CVE-2024-47431	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
16	Высокая	CVE-2024-49517	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
17	Высокая	CVE-2024-49525	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
18	Высокая	CVE-2024-47432	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
19	Высокая	CVE-2024-49520	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
20	Высокая	CVE-2024-47433	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
21	Высокая	CVE-2024-47434	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
22	Высокая	CVE-2024-49518	Adobe Substance 3D Painter	Локальный	ACE	2024-11-12	✓
23	Высокая	CVE-2024-47443	Adobe After Effects	Локальный	ACE	2024-11-12	✓
24	Высокая	CVE-2024-47442	Adobe After Effects	Локальный	ACE	2024-11-12	✓
25	Высокая	CVE-2024-47441	Adobe After Effects	Локальный	ACE	2024-11-12	✓
26	Средняя	CVE-2024-47456	Adobe Illustrator	Локальный	OSI	2024-11-12	✓
27	Высокая	CVE-2024-47452	Adobe Illustrator	Локальный	ACE	2024-11-12	✓
28	Высокая	CVE-2024-47451	Adobe Illustrator	Локальный	ACE	2024-11-12	✓

29	Высокая	CVE-2024-47450	Adobe Illustrator	Локальный	ACE	2024-11-12	✓
30	Высокая	CVE-2024-45114	Adobe Illustrator	Локальный	ACE	2024-11-12	✓
31	Высокая	CVE-2024-49509	Adobe InDesign	Локальный	ACE	2024-11-12	✓
32	Высокая	CVE-2024-49508	Adobe InDesign	Локальный	ACE	2024-11-12	✓
33	Высокая	CVE-2024-49507	Adobe InDesign	Локальный	ACE	2024-11-12	✓
34	Высокая	CVE-2024-10914	D-Link DNS-320, DNS-325 and DNS-340L NAS models	Сетевой	ACE	2024-11-11	✗
35	Высокая	CVE-2024-11115	Google Chrome и Microsoft Edge	Сетевой	OSI	2024-11-12	✓
36	Высокая	CVE-2024-11114	Google Chrome и Microsoft Edge	Сетевой	OSI	2024-11-12	✓
37	Высокая	CVE-2024-11113	Google Chrome и Microsoft Edge	Сетевой	OSI	2024-11-12	✓
38	Высокая	CVE-2024-11112	Google Chrome и Microsoft Edge	Сетевой	OSI	2024-11-12	✓
39	Высокая	CVE-2024-9712	Trimble SketchUp	Сетевой	ACE	2024-11-13	✗
40	Высокая	CVE-2024-9713	Trimble SketchUp Pro	Сетевой	ACE	2024-11-13	✗
41	Высокая	CVE-2024-9727	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✗
42	Высокая	CVE-2024-9720	Trimble SketchUp Viewer	Сетевой	OSI	2024-11-13	✗
43	Высокая	CVE-2024-9725	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✗

44	Высокая	CVE-2024-9724	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
45	Высокая	CVE-2024-9723	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
46	Высокая	CVE-2024-9722	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
47	Высокая	CVE-2024-9721	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
48	Высокая	CVE-2024-9714	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
49	Высокая	CVE-2024-9728	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
50	Высокая	CVE-2024-9731	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘
51	Высокая	CVE-2024-9726	Trimble SketchUp Viewer	Сетевой	ACE	2024-11-13	✘

Краткое описание: Выполнение произвольного кода в Microsoft

Идентификатор уязвимости: CVE-2024-49027

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024 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.

1 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49027>

Краткое описание: Выполнение произвольного кода в Microsoft

Идентификатор уязвимости: CVE-2024-49026

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Microsoft Office: 2019
Office Online Server : все версии
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024 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.

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:HI/H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49026>

Краткое описание: Получение конфиденциальной информации в Microsoft

Идентификатор уязвимости: CVE-2024-49028

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Office: 2019
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024 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.

3 **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: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49028>

Краткое описание: Выполнение произвольного кода в Microsoft

Идентификатор уязвимости: CVE-2024-49030

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

Уязвимый продукт: Microsoft Office: 2019
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024 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.

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49030>

Краткое описание: Выполнение произвольного кода в Microsoft

Идентификатор уязвимости: CVE-2024-49029

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Microsoft Office: 2019
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024 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:** 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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49029>

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-49514

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: Adobe Photoshop: с версии 24.0 по 25.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

- 6 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/photoshop/apsb24-89.html>

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

Идентификатор уязвимости: CVE-2024-49519

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Не определено

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47426

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47427

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47428

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47429

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47430

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-49515

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка 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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-49516

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47431

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

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-49517

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

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-49525

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

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47432

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

18 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-49520

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

19 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47433

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-47434

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

21 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

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

Идентификатор уязвимости: CVE-2024-49518

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: с версии 2.2 по 2021.1 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

22 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2024-47443

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: с версии 23.0 по 24.6.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb24-85.html

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2024-47442

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: с версии 23.0 по 24.6.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb24-85.html

Краткое описание: Выполнение произвольного кода в Adobe After Effects

Идентификатор уязвимости: CVE-2024-47441

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe After Effects: с версии 23.0 по 24.6.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

25 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://helpx.adobe.com/security/products/after_effects/apsb24-85.html

Краткое описание: Получение конфиденциальной информации в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-47456

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 5.5 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/illustrator/apsb24-87.html>

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-47452

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/illustrator/apsb24-87.html>

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-47451

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/illustrator/apsb24-87.html>

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-47450

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

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/illustrator/apsb24-87.html>

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-45114

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.7.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/illustrator/apsb24-87.html>

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-49509

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

Уязвимый продукт: Adobe InDesign: с версии 18.0 по 19.5

Категория уязвимого продукта: Не определено

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/indesign/apsb24-88.html>

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-49508

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

Уязвимый продукт: Adobe InDesign: с версии 18.0 по 19.5

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/indesign/apsb24-88.html>

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2024-49507

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

Уязвимый продукт: Adobe InDesign: с версии 18.0 по 19.5

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- <http://helpx.adobe.com/security/products/indesign/apsb24-88.html>

Краткое описание: Выполнение произвольного кода в D-Link DNS-320, DNS-325 and DNS-340L NAS models

Идентификатор уязвимости: CVE-2024-10914
BDU:2024-09234

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

Уязвимый продукт: D-Link DNS-320: с версии 1.00 по 1.10
D-Link DNS-320LW: все версии
D-Link DNS-325: все версии
D-Link DNS-340L: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная проверка входных данных.

34 **Последствия эксплуатации:** Выполнение произвольного кода

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

Оценка CVSSv3: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:HI:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-11-11 / 2024-11-11

Ссылки на источник:

- <http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10413>
- <http://netsecfish.notion.site/Command-Injection-Vulnerability-in-name-parameter-for-D-Link-NAS-12d6b683e67c80c49ffcc9214c239a07>
- <https://bdu.fstec.ru/vul/2024-09234>

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-11115

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Google Chrome и Microsoft Edge:
Google Chrome: 100.0.4896.60 - 130.0.6723.117
Microsoft Edge: 79.0.309.71 - 130.0.2849.80

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
- <http://crbug.com/371929521>

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-11114

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome и Microsoft Edge:
Google Chrome: 100.0.4896.60 - 130.0.6723.117
Microsoft Edge: 79.0.309.71 - 130.0.2849.80

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

36 **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:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
- <http://crbug.com/370856871>

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-11113

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome и Microsoft Edge:
Google Chrome: 100.0.4896.60 - 130.0.6723.117
Microsoft Edge: 79.0.309.71 - 130.0.2849.80

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
- <http://crbug.com/360274917>

Краткое описание: Получение конфиденциальной информации в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2024-11112

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome и Microsoft Edge:
Google Chrome: 100.0.4896.60 - 130.0.6723.117
Microsoft Edge: 79.0.309.71 - 130.0.2849.80

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Получение конфиденциальной информации

38 **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:H/PR:N/UI:R/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-12 / 2024-11-12

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop_12.html
- <http://crbug.com/354824998>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp

Идентификатор уязвимости: CVE-2024-9712

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Desktop: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1473/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Pro

Идентификатор уязвимости: CVE-2024-9713

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Pro: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

40 Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1474/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9727

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

41 Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1476/>

Краткое описание: Получение конфиденциальной информации в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9720

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

42 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1477/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9725

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

43 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1478/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9724

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

44 **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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1479/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9723

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

45 Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1480/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9722

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

46 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1481/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9721

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

47 **Рекомендации по устранению:** Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1482/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9714

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

48 Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевое 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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1483/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9728

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

49 **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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1484/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9731

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

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

50 **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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1485/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp Viewer

Идентификатор уязвимости: CVE-2024-9726

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: SketchUp Viewer for Windows: все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

51 **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: 2024-11-13 / 2024-11-13

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1475/>