НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-05-17.1 | 17 мая 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-32741	Siemens SIMATIC CN 4100	Сетевой	OSI	2024-05-17	✓
2	Критическая	CVE-2024-32740	Siemens SIMATIC CN 4100	Сетевой	ACE	2024-05-17	✓
3	Высокая	CVE-2024-31980	Siemens Parasolid	Локальный	ACE	2024-05-17	✓
4	Высокая	CVE-2024-32636	Siemens Parasolid	Локальный	OSI	2024-05-17	✓
5	Высокая	CVE-2024-32635	Siemens Parasolid	Локальный	OSI	2024-05-17	✓
6	Высокая	CVE-2024-20389	Cisco Crosswork Network Services Orchestrator	Локальный	PE	2024-05-16	✓
7	Высокая	CVE-2024-20326	Cisco Crosswork Network Services Orchestrator	Локальный	ACE	2024-05-16	✓
8	Высокая	CVE-2024-4948	Google Chrome	Сетевой	ACE	2024-05-16	✓
9	Высокая	CVE-2024-4947	Google Chrome	Сетевой	ACE	2024-05-16	✓
10	Высокая	CVE-2024-0801	Arcserve Unified Data Protection	Сетевой	DoS	2024-05-16	✓
11	Высокая	CVE-2024-0800	Arcserve Unified Data Protection	Сетевой	WLF	2024-05-16	✓
12	Критическая	CVE-2024-0799	Arcserve Unified Data Protection	Сетевой	SB	2024-05-16	✓
13	Высокая	CVE-2024-4367	Mozilla Firefox и Mozilla Thunderbird	Сетевой	ACE	2024-05-15	✓

14	Высокая	CVE-2024-4768	Mozilla Firefox	Сетевой	ACE	2024-05-15	✓
15	Высокая	CVE-2024-4764	Mozilla Firefox	Сетевой	ACE	2024-05-15	✓
16	Высокая	CVE-2024-4771	Mozilla Firefox	Сетевой	ACE	2024-05-15	✓
17	Высокая	CVE-2024-4777	Mozilla Firefox и Mozilla Thunderbird	Сетевой	ACE	2024-05-15	✓
18	Высокая	CVE-2024-4778	Mozilla Firefox	Сетевой	ACE	2024-05-15	✓
19	Высокая	CVE-2024-34100	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
20	Высокая	CVE-2024-34099	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
21	Высокая	CVE-2024-34098	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
22	Высокая	CVE-2024-34097	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
23	Высокая	CVE-2024-34096	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
24	Высокая	CVE-2024-34095	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
25	Высокая	CVE-2024-34094	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
26	Высокая	CVE-2024-30310	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
27	Высокая	CVE-2024-30284	Adobe Acrobat и Reader	Локальный	ACE	2024-05-15	✓
28	Критическая	CVE-2024-30314	Adobe Dreamweaver	Сетевой	ACE	2024-05-15	✓

29	Высокая	CVE-2024-30290	Adobe Framemaker	Локальный	ACE	2024-05-15	✓
30	Высокая	CVE-2024-30292	Adobe Framemaker	Локальный	ACE	2024-05-15	✓
31	Высокая	CVE-2024-30289	Adobe Framemaker	Локальный	ACE	2024-05-15	✓
32	Высокая	CVE-2024-30291	Adobe Framemaker	Локальный	ACE	2024-05-15	✓
33	Высокая	CVE-2024-30288	Adobe Framemaker	Локальный	ACE	2024-05-15	✓
34	Высокая	CVE-2024-20792	Adobe Illustrator	Локальный	ACE	2024-05-15	✓
35	Высокая	CVE-2024-20791	Adobe Illustrator	Локальный	ACE	2024-05-15	✓
36	Высокая	CVE-2024-30307	Adobe Substance 3D Painter	Локальный	ACE	2024-05-15	✓
37	Высокая	CVE-2024-30274	Adobe Substance 3D Painter	Локальный	ACE	2024-05-15	✓
38	Критическая	CVE-2024-34009	Moodle	Сетевой	SB	2024-05-15	✓
39	Высокая	CVE-2024-34005	Moodle	Сетевой	ACE	2024-05-15	✓
40	Высокая	CVE-2024-34004	Moodle	Сетевой	ACE	2024-05-15	✓
41	Высокая	CVE-2024-34003	Moodle	Сетевой	ACE	2024-05-15	✓
42	Высокая	CVE-2024-34002	Moodle	Сетевой	ACE	2024-05-15	✓
43	Критическая	CVE-2024-3044	LibreOffice	Сетевой	OSI	2024-05-15	✓

44	Высокая	CVE-2024-30042	Microsoft Excel	Локальный	ACE	2024-05-14	✓
45	Высокая	CVE-2024-4761	Microsoft Edge	Сетевой	ACE	2024-05-15	✓
46	Высокая	CVE-2024-30006	Microsoft WDAC OLE DB provider for SQL Server	Сетевой	ACE	2024-05-14	✓
47	Высокая	CVE-2024-30015	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
48	Высокая	CVE-2024-30029	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
49	Высокая	CVE-2024-30014	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
50	Высокая	CVE-2024-30022	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
51	Высокая	CVE-2024-30024	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
52	Высокая	CVE-2024-30023	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
53	Высокая	CVE-2024-30009	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2024-05-14	✓
54	Высокая	CVE-2024-30020	Microsoft Windows Cryptographic Services	Сетевой	ACE	2024-05-14	✓
55	Высокая	CVE-2024-30040	Microsoft Windows MSHTML platform	Сетевой	ACE	2024-05-14	✓
56	Высокая	CVE-2024-30051	Microsoft Windows DWM Core Library	Локальный	ACE	2024-05-14	✓

57	Высокая	CVE-2024-30045	Microsoft .NET and Visual Studio	Сетевой	ACE	2024-05-14	✓
58	Высокая	CVE-2024-4761	Google Chrome	Сетевой	ACE	2024-05-14	✓
59	Высокая	CVE-2024-27829	Apple macOS Sonoma	Сетевой	ACE	2024-05-14	✓
60	Критическая	CVE-2024-27818	Apple macOS Sonoma	Сетевой	ACE	2024-05-14	✓
61	Высокая	CVE-2024-27804	Apple macOS Sonoma	Локальный	ACE	2024-05-14	✓
62	Высокая	CVE-2024-27824	Apple macOS Sonoma	Локальный	PE	2024-05-14	✓
63	Высокая	CVE-2024-27813	Apple macOS Sonoma	Локальный	ACE	2024-05-14	✓
64	Высокая	CVE-2024-27843	Apple macOS Sonoma	Локальный	PE	2024-05-14	✓
65	Высокая	CVE-2024-27798	Apple macOS Sonoma	Локальный	PE	2024-05-14	✓
66	Высокая	CVE-2024-27842	Apple macOS Sonoma	Локальный	ACE	2024-05-14	✓
67	Высокая	CVE-2024-27796	Apple macOS Sonoma	Локальный	PE	2024-05-14	✓
68	Высокая	CVE-2024-27822	Apple macOS Sonoma	Локальный	PE	2024-05-14	✓
69	Высокая	CVE-2024-23296	Apple macOS Ventura	Локальный	ACE	2024-05-13	✓

1

Краткое описание: Получение конфиденциальной информации в Siemens SIMATIC CN 4100

Идентификатор уязвимости: CVE-2024-32741

Идентификатор программной ошибки: CWE-259 Использование жестко закодированного пароля

Уязвимый продукт: SIMATIC CN 4100: до 3.0

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-273900.html

2

Краткое описание: Выполнение произвольного кода в Siemens SIMATIC CN 4100

Идентификатор уязвимости: CVE-2024-32740

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

Уязвимый продукт: SIMATIC CN 4100: до 3.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-273900.html

3

Краткое описание: Выполнение произвольного кода в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-31980

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Parasolid: 35.1 - 36.1

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: 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: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-489698.html

4

Краткое описание: Получение конфиденциальной информации в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-32636

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Parasolid: 35.1 - 36.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-046364.html

5

Краткое описание: Получение конфиденциальной информации в Siemens Parasolid

Идентификатор уязвимости: CVE-2024-32635

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Parasolid: 35.1 - 36.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-05-17 / 2024-05-17

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-046364.html

6

Краткое описание: Повышение привилегий в Cisco Crosswork Network Services Orchestrator

Идентификатор уязвимости: CVE-2024-20389

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: Crosswork Network Services Orchestrator: 6.0 - 6.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-rwpesc-qrQGnh3f

7

Краткое описание: Выполнение произвольного кода в Cisco Crosswork Network Services Orchestrator

Идентификатор уязвимости: CVE-2024-20326

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

Уязвимый продукт: Crosswork Network Services Orchestrator: 5.1 - 6.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-rwpesc-qrQGnh3f

8

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4948

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.208

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.html
- http://crbug.com/333414294

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4947

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.208

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_15.html
- http://crbug.com/340221135

Краткое описание: Отказ в обслуживании в Arcserve Unified Data Protection

Идентификатор уязвимости: CVE-2024-0801

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Unified Data Protection: до 9.2 P00003050

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-07

Краткое описание: Запись локальных файлов в Arcserve Unified Data Protection

Идентификатор уязвимости: CVE-2024-0800

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Unified Data Protection: до 9.2 P00003050

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Запись локальных файлов

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-07

12

Краткое описание: Обход безопасности в Arcserve Unified Data Protection

Идентификатор уязвимости: CVE-2024-0799

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Unified Data Protection: до 9.2 P00003050

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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: 2024-05-16 / 2024-05-16

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-07
- https://bdu.fstec.ru/vul/2024-02247

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-4367

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Mozilla Firefox: 100.0 - 125.0.3
Firefox ESR: 102.0 - 115.10.0
Firefox for Android: 100.1.0 - 124.2.0
Mozilla Thunderbird: 102.0 - 115.10.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-22/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-23/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-4768

Идентификатор программной ошибки: CWE-357 Недостаточно очевидное предупреждение об опасных операциях

Уязвимый продукт: Mozilla Firefox: 100.0 - 125.0.3
Firefox ESR: 102.0 - 115.10.0
Firefox for Android: 100.1.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-22/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-4764

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 120.0 - 125.0.3
Firefox for Android: 120.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-4771

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 120.0 - 125.0.3
Firefox for Android: 120.0 - 124.2.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-4777

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 125.0.3
Firefox ESR: 102.0 - 115.10.0
Firefox for Android: 100.1.0 - 124.2.0
Mozilla Thunderbird: 102.0 - 115.10.2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-22/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-23/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2024-4778

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

Уязвимый продукт: Mozilla Firefox: 120.0 - 125.0.3
Firefox for Android: 120.0 - 124.2.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/

19

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34100

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

20

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34099

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

21

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34098

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34097

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

23

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34096

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

24

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34095

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

25

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-34094

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

26

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-30310

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

27

Краткое описание: Выполнение произвольного кода в Adobe Acrobat и Reader

Идентификатор уязвимости: CVE-2024-30284

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Reader и Adobe Acrobat:
Adobe Reader: 20.005.30331 - 2020.013.20074
Adobe Acrobat: 15.006.30306 - 24.002.20736

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/acrobat/apsb24-29.html

Краткое описание: Выполнение произвольного кода в Adobe Dreamweaver

Идентификатор уязвимости: CVE-2024-30314

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

Уязвимый продукт: Adobe Dreamweaver: 20.1 - 2019

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/dreamweaver/apsb24-39.html

29

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-30290

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Framemaker: с версии 2020.0 по 2022.3

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker/apsb24-37.html

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-30292

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Framemaker: с версии 2020.0 по 2022.3

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker/apsb24-37.html

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-30289

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Framemaker: с версии 2020.0 по 2022.3

Категория уязвимого продукта: Прикладное программное обеспечение

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker/apsb24-37.html

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-30291

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Framemaker: с версии 2020.0 по 2022.3

Категория уязвимого продукта: Прикладное программное обеспечение

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:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker/apsb24-37.html

33

Краткое описание: Выполнение произвольного кода в Adobe Framemaker

Идентификатор уязвимости: CVE-2024-30288

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

Уязвимый продукт: Adobe Framemaker: с версии 2020.0 по 2022.3

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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/framemaker/apsb24-37.html

34

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-20792

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.4.1

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: 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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb24-30.html

35

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2024-20791

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: с версии 22.0 по 28.4.1

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: 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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/illustrator/apsb24-30.html

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

Идентификатор уязвимости: CVE-2024-30307

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

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: 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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-31.html

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

Идентификатор уязвимости: CVE-2024-30274

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

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: 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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_painter/apsb24-31.html

38

Краткое описание: Обход безопасности в Moodle

Идентификатор уязвимости: CVE-2024-34009

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Moodle: 4.3.0 - 4.3.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=458398
- http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-81463

Краткое описание: Выполнение произвольного кода в Moodle

Идентификатор уязвимости: CVE-2024-34005

Идентификатор программной ошибки: CWE-98 Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP)

Уязвимый продукт: Moodle: 4.0.0 - 4.3.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

39 **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:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=458394
- http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-81267

Краткое описание: Выполнение произвольного кода в Moodle

Идентификатор уязвимости: CVE-2024-34004

Идентификатор программной ошибки: CWE-98 Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP)

Уязвимый продукт: Moodle: 4.0.0 - 4.3.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

40 **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:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=458393
- http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-81284

Краткое описание: Выполнение произвольного кода в Moodle

Идентификатор уязвимости: CVE-2024-34003

Идентификатор программной ошибки: CWE-98 Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP)

Уязвимый продукт: Moodle: 4.0.0 - 4.3.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

41 **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:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=458391
- http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-80712

Краткое описание: Выполнение произвольного кода в Moodle

Идентификатор уязвимости: CVE-2024-34002

Идентификатор программной ошибки: CWE-98 Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP)

Уязвимый продукт: Moodle: 4.0.0 - 4.3.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

42 **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:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=458390
- http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-81135

43

Краткое описание: Получение конфиденциальной информации в LibreOffice

Идентификатор уязвимости: CVE-2024-3044

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: LibreOffice: с версии 7.0.0.1 по 24.2.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://www.libreoffice.org/about-us/security/advisories/CVE-2024-3044

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2024-30042

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft Excel: 2016

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

44 **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: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30042

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-4761

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: с версии 79.0.309.71 до 124.0.2478.97

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

45 **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: 2024-05-15 / 2024-05-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-4761

Краткое описание: Выполнение произвольного кода в Microsoft WDAC OLE DB provider for SQL Server

Идентификатор уязвимости: CVE-2024-30006

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение пользователя к вредоносному SQL-серверу

Последствия эксплуатации: Выполнение произвольного кода

46

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: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30006

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30015

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

47

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30015

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30029

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

48

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30029

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30014

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

49

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30014

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30022

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

50

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30022

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30024

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

51

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30024

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30023

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

52

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:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30023

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2024-30009

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

53

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: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30009

Краткое описание: Выполнение произвольного кода в Microsoft Windows Cryptographic Services

Идентификатор уязвимости: CVE-2024-30020

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

54

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: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30020

55

Краткое описание: Выполнение произвольного кода в Microsoft Windows MSHTML platform

Идентификатор уязвимости: CVE-2024-30040

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Microsoft Internet Explorer: 11 - 11.1790.17763.0
Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Некорректная проверка входных 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: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30040

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

Идентификатор уязвимости: CVE-2024-30051

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

Уязвимый продукт: Windows: до 11 23H2 10.0.22631.3593
Windows Server: до 2022 10.0.20348.2461

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30051
- https://bdu.fstec.ru/vul/2024-03613

Краткое описание: Выполнение произвольного кода в Microsoft .NET and Visual Studio

Идентификатор уязвимости: CVE-2024-30045

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

Уязвимый продукт: Visual Studio: 2022 version 17.4 - 2022 version 17.9
.NET: 7.0.0 - 8.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

57

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30045

58

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4761

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.202

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_13.html
- http://crbug.com/339458194

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27829

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

59 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27818

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

60 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27804

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27824

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27813

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

64

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27843

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27798

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

66

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27842

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27796

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-27822

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

Уязвимый продукт: macOS: 14.0 23A344 - 14.4.1 23E224

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

68 **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:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-14 / 2024-05-14

Ссылки на источник:

- http://support.apple.com/en-us/HT214106

Краткое описание: Выполнение произвольного кода в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23296

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

Уязвимый продукт: macOS: 13.0 22A380 - 13.6.6 22G630

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-13 / 2024-05-13

Ссылки на источник:

- http://support.apple.com/en-us/HT214107
- https://bdu.fstec.ru/vul/2024-02552