НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-03-11.1 | 11 марта 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-23227	Apple macOS Ventura	Сетевой	OSI	2024-03-07	✓
2	Критическая	CVE-2024-23247	Apple macOS Ventura	Сетевой	ACE	2024-03-07	✓
3	Высокая	CVE-2024-23244	Apple macOS Ventura	Сетевой	PE	2024-03-07	✓
4	Высокая	CVE-2024-23270	Apple macOS Ventura	Локальный	PE	2024-03-07	✓
5	Критическая	CVE-2024-23286	Apple macOS Ventura	Сетевой	ACE	2024-03-07	✓
6	Критическая	CVE-2024-23257	Apple macOS Ventura	Сетевой	OSI	2024-03-07	✓
7	Высокая	CVE-2024-23234	Apple macOS Ventura	Локальный	PE	2024-03-07	✓
8	Высокая	CVE-2024-23265	Apple macOS Ventura	Локальный	PE	2024-03-07	✓
9	Высокая	CVE-2024-23225	Apple macOS Ventura	Локальный	ACE	2024-03-07	✓
10	Высокая	CVE-2024-23276	Apple macOS Ventura	Сетевой	PE	2024-03-07	✓
11	Высокая	CVE-2024-23201	Apple macOS Ventura	Сетевой	DoS	2024-03-07	✓
12	Высокая	CVE-2024-23283	Apple macOS Ventura	Сетевой	OSI	2024-03-07	✓
13	Критическая	CVE-2024-23274	Apple macOS Ventura	Сетевой	PE	2024-03-07	✓

14	Критическая	CVE-2024-23268	Apple macOS Ventura	Сетевой	PE	2024-03-07	✓
15	Высокая	CVE-2024-23275	Apple macOS Ventura	Сетевой	OSI	2024-03-07	✓
16	Критическая	CVE-2024-23267	Apple macOS Ventura	Сетевой	SB	2024-03-07	✓
17	Критическая	CVE-2024-23216	Apple macOS Ventura	Сетевой	ACE	2024-03-07	✓
18	Высокая	CVE-2024-23204	Apple macOS Ventura	Сетевой	OSI	2024-03-07	✓
19	Критическая	CVE-2024-23245	Apple macOS Ventura	Сетевой	SB	2024-03-07	✓
20	Высокая	CVE-2024-23272	Apple macOS Ventura	Сетевой	RLF	2024-03-07	✓
21	Высокая	CVE-2023-28826	Apple macOS	Сетевой	OSI	2024-03-07	✓
22	Высокая	None	Foxit PDF Editor for Mac	Сетевой	ACE	2024-03-08	✓
23	Критическая	CVE-2024-25858	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-03-08	✓
24	Высокая	CVE-2024-22167	Western Digital SanDisk PrivateAccess Desktop App for Windows	Локальный	ACE	2024-03-08	✓
25	Критическая	CVE-2024-23226	WebKitGTK+ и WPE WebKit	Сетевой	ACE	2024-03-07	✗
26	Высокая	CVE-2024-20337	Cisco Secure Client	Сетевой	ACE	2024-03-07	✓
27	Высокая	CVE-2024-2176	Google Chrome	Сетевой	ACE	2024-03-06	✓
28	Высокая	CVE-2024-2174	Google Chrome	Сетевой	OSI	2024-03-06	✓

29	Высокая	CVE-2024-22667	Vim	Локальный	ACE	2024-03-07	✓
30	Высокая	CVE-2024-20337	Cisco Secure Client	Сетевой	ACE	2024-03-07	✓
31	Высокая	CVE-2024-2173	Google Chrome	Сетевой	ACE	2024-03-06	✓
32	Высокая	CVE-2024-1220	Moxa NPort W2150A/W2250A Series	Сетевой	DoS	2024-03-06	✓
33	Высокая	CVE-2024-22254	VMware ESXi	Локальный	PE	2024-03-05	✓
34	Критическая	CVE-2024-22253	VMware ESXi, VMware Workstation and Fusion	Локальный	ACE	2024-03-05	✓
35	Критическая	CVE-2024-22252	VMware ESXi, VMware Workstation and Fusion	Локальный	ACE	2024-03-05	✓
36	Высокая	CVE-2024-22243	Rundeck	Сетевой	CSRF	2024-03-05	✓
37	Высокая	CVE-2024-27199	JetBrains TeamCity	Сетевой	SB	2024-03-05	✓
38	Критическая	CVE-2024-27198	JetBrains TeamCity	Сетевой	SB	2024-03-05	✓
39	Высокая	CVE-2024-27337	Kofax Power PDF Advanced	Сетевой	ACE	2024-03-04	✓
40	Высокая	CVE-2024-27339	Kofax Power PDF Advanced	Сетевой	ACE	2024-03-04	✓
41	Высокая	CVE-2024-27344	Kofax Power PDF Advanced	Сетевой	ACE	2024-03-04	✓
42	Высокая	CVE-2024-27342	Kofax Power PDF Advanced	Сетевой	ACE	2024-03-04	✓
43	Высокая	CVE-2024-27341	Kofax Power PDF Advanced	Сетевой	ACE	2024-03-04	✓

44	Высокая	CVE-2024-27340	Kofax Power PDF Advanced	Сетевой	ACE	2024-03-04	✓
45	Высокая	CVE-2024-27338	Kofax Power PDF Advanced	Сетевой	OSI	2024-03-04	✓
46	Высокая	CVE-2024-27335	Kofax Power PDF Advanced	Сетевой	OSI	2024-03-04	✓
47	Критическая	CVE-2024-27139	Apache Archiva	Сетевой	SB	2024-03-04	✗
48	Критическая	CVE-2024-1597	PostgreSQL JDBC driver, Openfire, Rundeck	Сетевой	ACE	2024-03-04	✓

1

Краткое описание: Получение конфиденциальной информации в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23227

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

2

Краткое описание: Выполнение произвольного кода в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23247

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple 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: 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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

3

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23244

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

4

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23270

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

5

Краткое описание: Выполнение произвольного кода в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23286

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple 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: 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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

6

Краткое описание: Получение конфиденциальной информации в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23257

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

7

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23234

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

8

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23265

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

Краткое описание: Выполнение произвольного кода в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23225

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

Уязвимый продукт: macOS: с версии 13.0 22A380 по 13.6.4 22G513

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

10

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23276

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

Краткое описание: Отказ в обслуживании в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23201

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.3
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: отказ в обслуживании

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

Краткое описание: Получение конфиденциальной информации в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23283

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

13

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23274

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

14

Краткое описание: Повышение привилегий в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23268

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

15

Краткое описание: Получение конфиденциальной информации в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23275

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 8.1 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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

16

Краткое описание: Обход безопасности в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23267

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

17

Краткое описание: Выполнение произвольного кода в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23216

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

Краткое описание: Получение конфиденциальной информации в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23204

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS: Sonoma до 14.3

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

19

Краткое описание: Обход безопасности в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23245

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

Краткое описание: Чтение локальных файлов в Apple macOS Ventura

Идентификатор уязвимости: CVE-2024-23272

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

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.4
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

20 **Последствия эксплуатации:** чтение локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

Краткое описание: Получение конфиденциальной информации в Apple macOS

Идентификатор уязвимости: CVE-2023-28826

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: macOS: Monterey до 12.7.4
macOS: Sonoma до 14.1
macOS: Ventura до 13.6.5

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214085

22

Краткое описание: Выполнение произвольного кода в Foxit PDF Editor for Mac

Идентификатор уязвимости: None

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

Уязвимый продукт: Foxit PDF Editor for Mac (formerly PhantomPDF): до версии 2024.1.0.63682

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-08 / 2024-03-08

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+for+Mac+2024.1+and+Foxit+PDF+Reader+for+Mac+2024.12024-03-05+00%3A00%3A00

23

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

Идентификатор уязвимости: CVE-2024-25858

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

Уязвимый продукт: Foxit PDF Reader: для Windows с версии 10.0.0.35798 по 2023.3.0.23028

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: 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: 2024-03-08 / 2024-03-08

Ссылки на источник:

- http://www.foxit.com/support/security-bulletins.html

Краткое описание: Выполнение произвольного кода в Western Digital SanDisk PrivateAccess Desktop App for Windows

Идентификатор уязвимости: CVE-2024-22167

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: SanDisk PrivateAccess Desktop App for Windows: до версии 6.4.10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

2
4

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: 2024-03-08 / 2024-03-08

Ссылки на источник:

- http://www.westerndigital.com/support/product-security/wdc-24002-sandisk-privateaccess-desktop-app-v-6-4-10

25

Краткое описание: Выполнение произвольного кода в WebKitGTK+ и WPE WebKit

Идентификатор уязвимости: CVE-2024-23226

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

Уязвимый продукт: WPE WebKit и WebKitGTK: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Последствия эксплуатации: выполнение произвольного кода

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

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: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://support.apple.com/en-us/HT214084

26

Краткое описание: Выполнение произвольного кода в Cisco Secure Client

Идентификатор уязвимости: CVE-2024-20337

Идентификатор программной ошибки: CWE-93 Некорректная нейтрализация последовательностей символов CRLF (внедрение символов CRLF)

Уязвимый продукт: Cisco Secure Client: с версии 4.10.04065 по 5.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7

27

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-2176

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 122.0.6261.96

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-06 / 2024-03-06

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html
- http://crbug.com/325936438

28

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-2174

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 122.0.6261.96

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-06 / 2024-03-06

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html
- http://crbug.com/325866363

29

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2024-22667

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Vim: с версии 9.0.0000 по 9.0.2141

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:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://github.com/vim/vim/commit/b39b240c386a5a29241415541f1c99e2e6b8ce47
- http://gist.githubusercontent.com/henices/2467e7f22dcc2aa97a2453e197b55a0c/raw/7b54bccc9a129c604fb139266f4497ab7aaa94c7/gistfile1.txt

30

Краткое описание: Выполнение произвольного кода в Cisco Secure Client

Идентификатор уязвимости: CVE-2024-20337

Идентификатор программной ошибки: CWE-93 Некорректная нейтрализация последовательностей символов CRLF (внедрение символов CRLF)

Уязвимый продукт: Cisco Secure Client: с версии 4.10.04065 по 5.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-07 / 2024-03-07

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7

31

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-2173

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 122.0.6261.96

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-06 / 2024-03-06

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop.html
- http://crbug.com/325893559

Краткое описание: Отказ в обслуживании в Moxa NPort W2150A/W2250A Series

Идентификатор уязвимости: CVE-2024-1220

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: NPort W2150A: 2.3
NPort W2250A: 2.3

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: отказ в обслуживании

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-06 / 2024-03-06

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mpsa-238975-nport-w2150a-w2250a-series-web-server-stack-based-buffer-overflow-vulnerability
- https://bdu.fstec.ru/vul/2024-01811

Краткое описание: Повышение привилегий в VMware ESXi

Идентификатор уязвимости: CVE-2024-22254

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMware ESXi: до ESXi80U2sb-23305545

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

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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

Оценка CVSSv3: 7.9 AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-05 / 2024-03-05

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2024-0006.html
- https://bdu.fstec.ru/vul/2024-01810

3
4

Краткое описание: Выполнение произвольного кода в VMware ESXi, VMware Workstation and Fusion

Идентификатор уязвимости: CVE-2024-22253

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: VMware ESXi: до ESXi80U2sb-23305545
VMware Fusion: 13.0 - 13.5
VMware Workstation: 17.0 - 17.5

Категория уязвимого продукта: Unix-подобные операционные системы 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: 9.3 AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-05 / 2024-03-05

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2024-0006.html
- https://bdu.fstec.ru/vul/2024-01808

35

Краткое описание: Выполнение произвольного кода в VMware ESXi, VMware Workstation and Fusion

Идентификатор уязвимости: CVE-2024-22252

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: VMware ESXi: до ESXi80U2sb-23305545
VMware Fusion: 13.0 - 13.5
VMware Workstation: 17.0 - 17.5

Категория уязвимого продукта: Unix-подобные операционные системы 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: 9.3 AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-05 / 2024-03-05

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2024-0006.html
- https://bdu.fstec.ru/vul/2024-01807

Краткое описание: Подделка запросов на стороне сервера в Rundeck

Идентификатор уязвимости: CVE-2024-22243

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: Rundeck: 4.17.0 - 4.17.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: подделка запросов на стороне сервера

3
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: 8.1 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: 2024-03-05 / 2024-03-05

Ссылки на источник:

- http://github.com/rundeck/rundeck/releases/tag/v4.17.5
- https://bdu.fstec.ru/vul/2024-01709

37

Краткое описание: Обход безопасности в JetBrains TeamCity

Идентификатор уязвимости: CVE-2024-27199

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: TeamCity: 3.1 - 2023.11.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса авторизации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-05 / 2024-03-05

Ссылки на источник:

- http://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/

38

Краткое описание: Обход безопасности в JetBrains TeamCity

Идентификатор уязвимости: CVE-2024-27198

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: TeamCity: 3.1 - 2023.11.3

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: 2024-03-05 / 2024-03-05

Ссылки на источник:

- http://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/
- https://bdu.fstec.ru/vul/2024-01792

39

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27337

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-230/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

40

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27339

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-231/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

41

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27344

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

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-224/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

42

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27342

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-222/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

43

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27341

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

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

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:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-221/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

Краткое описание: Выполнение произвольного кода в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27340

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

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

4
4 **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: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-220/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

Краткое описание: Получение конфиденциальной информации в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27338

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: получение конфиденциальной информации

4
5 **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: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-219/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

Краткое описание: Получение конфиденциальной информации в Kofax Power PDF Advanced

Идентификатор уязвимости: CVE-2024-27335

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Power PDF Advanced: до 5.0.0.17

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: получение конфиденциальной информации

4
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: 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: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-217/
- http://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.17.htm

47

Краткое описание: Обход безопасности в Apache Archiva

Идентификатор уязвимости: CVE-2024-27139

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Apache Archiva: 2.0.0 - 2.2.10

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://lists.apache.org/thread/qr8b7r86p1hkn0dc0q827s981kf1bgd8

Краткое описание: Выполнение произвольного кода в PostgreSQL JDBC driver, Openfire, Rundeck

Идентификатор уязвимости: CVE-2024-1597

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: Postgresql JDBC Driver: 42.0.0 - 42.7.1
Openfire: 4.8.0
Rundeck: 4.17.0 - 5.1.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: выполнение произвольного кода

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

4
8

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: 2024-03-04 / 2024-03-04

Ссылки на источник:

- http://github.com/pgjdbc/pgjdbc/security/advisories/GHSA-24rp-q3w6-vc56
- http://www.enterprisedb.com/docs/security/assessments/cve-2024-1597/
- http://www.enterprisedb.com/docs/jdbc_connector/latest/01_jdbc_rel_notes/
- http://github.com/igniterealtime/Openfire/releases/tag/v4.8.1
- http://github.com/rundeck/rundeck/releases/tag/v4.17.5
- http://github.com/rundeck/rundeck/releases/tag/v5.1.1
- https://bdu.fstec.ru/vul/2024-01541