НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-01-24.1 | 24 января 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-23210	Apple macOS Sonoma	Сетевой	OSI	2024-01-22	✓
2	Высокая	CVE-2024-23215	Apple macOS Sonoma	Сетевой	SB	2024-01-22	✓
3	Критическая	CVE-2024-23224	Apple macOS Sonoma	Сетевой	OSI	2024-01-22	✓
4	Высокая	CVE-2024-23208	Apple macOS Sonoma	Локальный	PE	2024-01-22	✓
5	Критическая	CVE-2024-23209	Apple macOS Sonoma	Сетевой	ACE	2024-01-22	✓
6	Высокая	CVE-2024-23207	Apple macOS Sonoma	Сетевой	OSI	2024-01-22	✓
7	Высокая	CVE-2024-23223	Apple macOS Sonoma	Сетевой	OSI	2024-01-22	✓
8	Критическая	CVE-2021-42575	Hyperion Planning	Сетевой	ACE	2024-01-18	✓
9	Высокая	CVE-2023-5072	Hyperion Planning	Сетевой	DoS	2024-01-18	✓
10	Критическая	CVE-2023-50164	Infrastructure Technology	Сетевой	ACE	2024-01-18	✓
11	Высокая	CVE-2024-23212	Apple macOS Sonoma	Локальный	PE	2024-01-22	✓
12	Критическая	CVE-2024-23203	Apple macOS Sonoma	Сетевой	OSI	2024-01-22	✓
13	Высокая	CVE-2022-46751	Oracle Business Intelligence Enterprise Edition	Сетевой	OSI	2024-01-18	✓

14	Высокая	CVE-2023-39410	Oracle Business Intelligence Enterprise Edition	Сетевой	DoS	2024-01-18	✓
15	Высокая	CVE-2021-33813	Oracle Business Intelligence Enterprise Edition	Сетевой	OSI	2024-01-18	✓
16	Высокая	CVE-2022-3510	Oracle Business Intelligence Enterprise Edition	Сетевой	DoS	2024-01-18	✓
17	Высокая	CVE-2022-25647	Oracle Business Intelligence Enterprise Edition	Сетевой	DoS	2024-01-18	✓
18	Высокая	CVE-2023-38039	Apple macOS Monterey	Сетевой	DoS	2024-01-22	✓
19	Высокая	CVE-2023-43642	Oracle Business Intelligence Enterprise Edition	Сетевой	DoS	2024-01-18	✓
20	Высокая	CVE-2023-42937	Apple macOS Ventura	Сетевой	OSI	2024-01-22	✓
21	Критическая	CVE-2024-23204	Apple macOS Sonoma	Сетевой	OSI	2024-01-22	✓
22	Критическая	CVE-2022-36944	Oracle Communications BRM - Elastic Charging Engine	Сетевой	ACE	2024-01-19	✓
23	Высокая	CVE-2023-51552	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
24	Высокая	CVE-2023-32616	Foxit PDF Editor for Windows	Сетевой	ACE	2024-01-22	✓
25	Высокая	CVE-2023-41257	Foxit PDF Editor for Windows	Сетевой	ACE	2024-01-22	✓
26	Высокая	CVE-2023-38573	Foxit PDF Editor for Windows	Сетевой	ACE	2024-01-22	✓
27	Высокая	CVE-2023-51556	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓

28	Высокая	CVE-2023-51557	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
29	Высокая	CVE-2023-51551	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
30	Высокая	CVE-2023-51549	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
31	Высокая	CVE-2023-35985	Foxit PDF Editor for Windows	Сетевой	ACE	2024-01-22	✓
32	Высокая	CVE-2023-51560	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
33	Высокая	CVE-2023-42091	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
34	Высокая	CVE-2023-42092	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
35	Высокая	CVE-2023-42094	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
36	Высокая	CVE-2023-42096	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
37	Высокая	CVE-2023-42097	Foxit PDF Editor for Windows	Локальный	ACE	2024-01-22	✓
38	Высокая	CVE-2023-39542	Foxit PDF Editor for Windows	Сетевой	ACE	2024-01-22	✓
39	Высокая	CVE-2023-40194	Foxit PDF Editor for Windows	Сетевой	ACE	2024-01-22	✓
40	Критическая	CVE-2024-22916	D-Link GO-RT-AC750	Сетевой	ACE	2024-01-22	✗
41	Высокая	CVE-2024-21733	Apache Tomcat	Сетевой	OSI	2024-01-19	✓
42	Высокая	CVE-2024-23206	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2024-01-22	✗

43	Высокая	CVE-2024-23213	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2024-01-22	✗
44	Высокая	CVE-2024-23214	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2024-01-22	✗
45	Высокая	CVE-2024-23222	WebKitGTK+ and WPE WebKit	Сетевой	ACE	2024-01-22	✗
46	Высокая	CVE-2024-22421	JupyterLab	Сетевой	RLF	2024-01-23	✓
47	Критическая	CVE-2024-0755	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-01-23	✓
48	Критическая	CVE-2024-0743	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-01-23	✓
49	Критическая	CVE-2024-0745	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-01-23	✓
50	Критическая	CVE-2024-0741	Mozilla Firefox and Firefox ESR	Сетевой	ACE	2024-01-23	✓
51	Критическая	CVE-2024-0751	Mozilla Thunderbird	Сетевой	PE	2024-01-23	✓
52	Критическая	CVE-2023-49657	Apache Superset	Сетевой	XSS\CSS	2024-01-23	✓
53	Высокая	CVE-2023-6926	Crestron AM-300	Локальный	OSI	2024-01-24	✓
54	Высокая	CVE-2024-0806	Google Chrome	Сетевой	OSI	2024-01-23	✓
55	Высокая	CVE-2024-0813	Google Chrome	Сетевой	OSI	2024-01-23	✓
56	Высокая	CVE-2024-0808	Google Chrome	Сетевой	ACE	2024-01-23	✓
57	Высокая	CVE-2024-0812	Google Chrome	Сетевой	OSI	2024-01-23	✓

58	Высокая	CVE-2024-0807	Google Chrome	Сетевой	ACE	2024-01-23	✓
59	Критическая	CVE-2023-51984	D-Link DIR-822	Сетевой	ACE	2024-01-11	✓
60	Высокая	CVE-2024-0543	Tenda W9	Сетевой	DoS	2024-01-15	✓
61	Высокая	CVE-2024-21616	Juniper Junos OS	Сетевой	DoS	2024-01-10	✓
62	Высокая	CVE-2024-21612	Junos OS	Сетевой	DoS	2024-01-10	✓
63	Высокая	CVE-2024-21614	Junos OS	Сетевой	DoS	2024-01-10	✓
64	Высокая	CVE-2024-21611	Junos OS	Сетевой	DoS	2024-01-11	✓
65	Высокая	CVE-2024-21606	Juniper Junos OS	Сетевой	DoS	2024-01-10	✓
66	Высокая	CVE-2024-21595	Juniper Junos OS	Сетевой	DoS	2024-01-10	✓
67	Высокая	CVE-2023-44250	FortiOS and FortiProxy	Сетевой	ACE	2024-01-09	✓
68	Критическая	CVE-2024-21591	Juniper Junos OS	Сетевой	ACE	2024-01-10	✓
69	Высокая	CVE-2024-21602	Junos OS	Сетевой	DoS	2024-01-10	✓
70	Высокая	CVE-2024-21604	Junos OS	Сетевой	DoS	2024-01-10	✓

1

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23210

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

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

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:N/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

2

Краткое описание: Обход безопасности в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23215

Идентификатор программной ошибки: CWE-377 Уязвимости, связанные с небезопасными временными файлами

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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: 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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23224

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

4

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23208

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

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

5

Краткое описание: Выполнение произвольного кода в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23209

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

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

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: 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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

6

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23207

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

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23223

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

8

Краткое описание: Выполнение произвольного кода в Hyperion Planning

Идентификатор уязвимости: CVE-2021-42575

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Hyperion Planning: версии 11.2.14.0.000

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

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: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?505632

Краткое описание: Отказ в обслуживании в Hyperion Planning

Идентификатор уязвимости: CVE-2023-5072

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Hyperion Planning: версии 11.2.14.0.000

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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: 7.5 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: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?505632

10

Краткое описание: Выполнение произвольного кода в Infrastructure Technology

Идентификатор уязвимости: CVE-2023-50164

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

Уязвимый продукт: Infrastructure Technology: версии 11.2.14.0.000

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка 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: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?917626
- https://bdu.fstec.ru/vul/2023-08547

Краткое описание: Повышение привилегий в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23212

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

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23203

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

Краткое описание: Получение конфиденциальной информации в Oracle Business Intelligence Enterprise Edition

Идентификатор уязвимости: CVE-2022-46751

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Oracle Business Intelligence Enterprise Edition: версии 6.4.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3222

14

Краткое описание: Отказ в обслуживании в Oracle Business Intelligence Enterprise Edition

Идентификатор уязвимости: CVE-2023-39410

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Oracle Business Intelligence Enterprise Edition: с версии 6.4.0.0.0 по 7.0.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3222

15

Краткое описание: Получение конфиденциальной информации в Oracle Business Intelligence Enterprise Edition

Идентификатор уязвимости: CVE-2021-33813

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Oracle Business Intelligence Enterprise Edition: версии 6.4.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3222

16

Краткое описание: Отказ в обслуживании в Oracle Business Intelligence Enterprise Edition

Идентификатор уязвимости: CVE-2022-3510

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Oracle Business Intelligence Enterprise Edition: с версии 6.4.0.0.0 по 7.0.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3222
- https://bdu.fstec.ru/vul/2023-04975

17

Краткое описание: Отказ в обслуживании в Oracle Business Intelligence Enterprise Edition

Идентификатор уязвимости: CVE-2022-25647

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Oracle Business Intelligence Enterprise Edition: с версии 6.4.0.0.0 по 7.0.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3222
- https://bdu.fstec.ru/vul/2023-09014

18

Краткое описание: Отказ в обслуживании в Apple macOS Monterey

Идентификатор уязвимости: CVE-2023-38039

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: macOS: с версии 12.0 21A344 по 12.7.2 21G1974

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214057
- https://bdu.fstec.ru/vul/2023-05819

Краткое описание: Отказ в обслуживании в Oracle Business Intelligence Enterprise Edition

Идентификатор уязвимости: CVE-2023-43642

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Oracle Business Intelligence Enterprise Edition: версии 7.0.0.0.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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

Оценка CVSSv3: 7.5 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: 2024-01-18 / 2024-01-18

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?3222

Краткое описание: Получение конфиденциальной информации в Apple macOS Ventura

Идентификатор уязвимости: CVE-2023-42937

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

Уязвимый продукт: macOS: 13.0 22A380 - 13.6.3 22G436

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214058

Краткое описание: Получение конфиденциальной информации в Apple macOS Sonoma

Идентификатор уязвимости: CVE-2024-23204

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: macOS: с версии 14.0 23A344 по 14.2.1 23C71

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Обход ограничений безопасности

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: 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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

22

Краткое описание: Выполнение произвольного кода в Oracle Communications BRM - Elastic Charging Engine

Идентификатор уязвимости: CVE-2022-36944

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Oracle Communications BRM - Elastic Charging Engine: с версии 12.0.0.4 по 12.0.0.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-01-19 / 2024-01-19

Ссылки на источник:

- http://www.oracle.com/security-alerts/cpujan2024.html?904649
- https://bdu.fstec.ru/vul/2023-00169

23

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

Идентификатор уязвимости: CVE-2023-51552

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): 11.0.0.0510 - 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-09052

24

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

Идентификатор уязвимости: CVE-2023-32616

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-08381

25

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

Идентификатор уязвимости: CVE-2023-41257

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-08377

26

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

Идентификатор уязвимости: CVE-2023-38573

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-08378

27

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

Идентификатор уязвимости: CVE-2023-51556

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 - 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-09048

28

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

Идентификатор уязвимости: CVE-2023-51557

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-09054

29

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

Идентификатор уязвимости: CVE-2023-51551

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-09053

30

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

Идентификатор уязвимости: CVE-2023-51549

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2024-00053

31

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

Идентификатор уязвимости: CVE-2023-35985

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00

32

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

Идентификатор уязвимости: CVE-2023-51560

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

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00

33

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

Идентификатор уязвимости: CVE-2023-42091

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-05918

34

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

Идентификатор уязвимости: CVE-2023-42092

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-06081

35

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

Идентификатор уязвимости: CVE-2023-42094

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00

36

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

Идентификатор уязвимости: CVE-2023-42096

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00

37

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

Идентификатор уязвимости: CVE-2023-42097

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00

38

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

Идентификатор уязвимости: CVE-2023-39542

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-08380

39

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

Идентификатор уязвимости: CVE-2023-40194

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 - 12.1.3.15356

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00
- https://bdu.fstec.ru/vul/2023-08379

40

Краткое описание: Выполнение произвольного кода в D-Link GO-RT-AC750

Идентификатор уязвимости: CVE-2024-22916

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Go-RT-AC750: версии 101b03

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://www.dlink.com/en/security-bulletin/
- http://kee02p.github.io/2024/01/13/CVE-2024-22916/

41

Краткое описание: Получение конфиденциальной информации в Apache Tomcat

Идентификатор уязвимости: CVE-2024-21733

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

Уязвимый продукт: Apache Tomcat: с версии 8.5.0 по 9.0.43

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2024-01-19 / 2024-01-19

Ссылки на источник:

- http://lists.apache.org/thread/h9bjqdd0odj6lhs2o96qgowcc6hb0cfz
- http://www.openwall.com/lists/oss-security/2024/01/19/2

42

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

Идентификатор уязвимости: CVE-2024-23206

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

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально 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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

43

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

Идентификатор уязвимости: CVE-2024-23213

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

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально 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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

44

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

Идентификатор уязвимости: CVE-2024-23214

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

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

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально 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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

45

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

Идентификатор уязвимости: CVE-2024-23222

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

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: 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: 8.8 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-22 / 2024-01-22

Ссылки на источник:

- http://support.apple.com/en-us/HT214061

46

Краткое описание: Чтение локальных файлов в JupyterLab

Идентификатор уязвимости: CVE-2024-22421

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

Уязвимый продукт: JupyterLab: с версии 3.6.0 по 4.0.9

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://github.com/jupyterlab/jupyterlab/security/advisories/GHSA-44cc-43rp-5947
- http://github.com/jupyterlab/jupyterlab/commit/19bd9b96cb2e77170a67e43121637d0b5619e8c6

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-0755

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

Уязвимый продукт: Mozilla Firefox: с версии 100.0 по 121.0.1
Firefox ESR: с версии 102.0 по 115.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-01/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-02/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-0743

Идентификатор программной ошибки: CWE-252 Отсутствует проверка возвращаемых значений

Уязвимый продукт: Mozilla Firefox: с версии 116.0 по 121.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-01/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-0745

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Mozilla Firefox: с версии 116.0 по 121.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-01/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox and Firefox ESR

Идентификатор уязвимости: CVE-2024-0741

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Mozilla Firefox: с версии 100.0 по 121.0.1
Firefox ESR: с версии 102.0 по 115.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-01/
- http://www.mozilla.org/en-US/security/advisories/mfsa2024-02/

Краткое описание: Повышение привилегий в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-0751

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

Уязвимый продукт: Mozilla Thunderbird: с версии 102.0 по 115.6.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий

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: 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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://www.mozilla.org/en-US/security/advisories/mfsa2024-04/

Краткое описание: Межсайтовый скриптинг в Apache Superset

Идентификатор уязвимости: CVE-2023-49657

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: Apache Superset: с версии 3.0.0 по 3.0.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: межсайтовый скриптинг

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://lists.apache.org/thread/wjyvz8om9nwd396lh0bt156mtwjxpsvx

Краткое описание: Получение конфиденциальной информации в Crestron AM-300

Идентификатор уязвимости: CVE-2023-6926

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: Crestron AM-300: версии 1.4499.00018

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: получение конфиденциальной информации

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: 8.4 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: 2024-01-24 / 2024-01-24

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-023-02

54

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-0806

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 120.0.6099.225

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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
- http://crbug.com/1505176

55

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-0813

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 120.0.6099.225

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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
- http://crbug.com/1477151

56

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-0808

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 120.0.6099.225

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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
- http://crbug.com/1504936

57

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-0812

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 120.0.6099.225

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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
- http://crbug.com/1484394

58

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-0807

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 120.0.6099.225

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: 2024-01-23 / 2024-01-23

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html
- http://crbug.com/1505080

Краткое описание: Выполнение произвольного кода в D-Link DIR-822

Идентификатор уязвимости: CVE-2023-51984

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

Уязвимый продукт: D-Link DIR-822: до версии V1.0.2.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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: 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: 2024-01-11 / 2024-01-18

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-51984

Краткое описание: Отказ в обслуживании в Tenda W9

Идентификатор уязвимости: CVE-2024-0543

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

Уязвимый продукт: Tenda W9: до версии 1.0.0.7.

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: отказ в обслуживании

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: 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: 2024-01-15 / 2024-01-22

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2024-0543

61

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21616

Идентификатор программной ошибки: CWE-1286 Некорректная проверка правильности синтаксиса входных данных

Уязвимый продукт: Juniper Junos OS: серии MX и SRX до версии 23.2R2

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

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-Processing-of-a-specific-SIP-packet-causes-NAT-IP-allocation-to-fail-CVE-2024-21616
- https://bdu.fstec.ru/vul/2024-00396

62

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-21612

Идентификатор программной ошибки: CWE-228 Некорректная обработка синтаксически неверных структур

Уязвимый продукт: Junos OS: до версии 22.4R2.

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

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-Evolved-Specific-TCP-traffic-causes-OFP-core-and-restart-of-RE-CVE-2024-21612
- https://bdu.fstec.ru/vul/2024-00398

63

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-21614

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Junos OS: до версии 22.2R1.

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

Способ эксплуатации: Отправка специально сформированного запроса.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-specific-query-via-DREND-causes-rpd-crash-CVE-2024-21614
- https://bdu.fstec.ru/vul/2024-00399

64

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-21611

Идентификатор программной ошибки: CWE-401 Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)

Уязвимый продукт: Junos OS : до версии 22.2R2

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

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-11 / 2024-01-11

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-jflow-scenario-continuous-route-churn-will-cause-a-memory-leak-and-eventually-an-rpd-crash-CVE-2024-21611
- https://bdu.fstec.ru/vul/2024-00395

65

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21606

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Juniper Junos OS: до версии 22.4R2

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

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-flowd-will-crash-when-tcp-encap-is-enabled-and-specific-packets-are-received-CVE-2024-21606
- https://bdu.fstec.ru/vul/2024-00397

66

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21595

Идентификатор программной ошибки: CWE-1286 Некорректная проверка правильности синтаксиса входных данных

Уязвимый продукт: Juniper Junos OS: до версии 23.1R2

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

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-EX4100-EX4400-EX4600-and-QFX5000-Series-A-high-rate-of-specific-ICMP-traffic-will-cause-the-PFE-to-hang-CVE-2024-21595
- https://bdu.fstec.ru/vul/2024-00445

67

Краткое описание: Выполнение произвольного кода в FortiOS and FortiProxy

Идентификатор уязвимости: CVE-2023-44250

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: FortiOS и FortiProxy: до версии 7.4.1

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

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-09 / 2024-01-09

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-23-315
- https://bdu.fstec.ru/vul/2024-00117

68

Краткое описание: Выполнение произвольного кода в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-21591

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Juniper Junos OS: до версии 22.4R2

Категория уязвимого продукта: Unix-подобные операционные системы 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: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591
- https://bdu.fstec.ru/vul/2024-00263

69

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-21602

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Junos OS: до версии 22.3R2

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

Способ эксплуатации: Отправка специально сформированного запроса.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-Evolved-ACX7024-ACX7100-32C-and-ACX7100-48L-Traffic-stops-when-a-specific-IPv4-UDP-packet-is-received-by-the-RE-CVE-2024-21602
- https://bdu.fstec.ru/vul/2024-00394

70

Краткое описание: Отказ в обслуживании в Junos OS

Идентификатор уязвимости: CVE-2024-21604

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: Junos OS: до версии 22.4R1

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

Способ эксплуатации: Отправка специально сформированных данных.

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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-01-10 / 2024-01-10

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-Evolved-A-high-rate-of-specific-traffic-will-cause-a-complete-system-outage-CVE-2024-21604
- https://bdu.fstec.ru/vul/2024-00393