НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-08-30.1 | 30 августа 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-40619	Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix and Compact GuardLogix 5380	Сетевой	DoS	2024-08-26	✓
2	Высокая	CVE-2024-7515	Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix and Compact GuardLogix 5380	Сетевой	DoS	2024-08-26	✓
3	Высокая	CVE-2024-7507	Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix and Compact GuardLogix 5380	Сетевой	DoS	2024-08-26	✓
4	Высокая	CVE-2024-7977	Microsoft Edge	Локальный	OSI	2024-08-23	✓
5	Высокая	CVE-2024-41879	Microsoft Edge	Локальный	ACE	2024-08-23	✓
6	Высокая	CVE-2024-38210	Microsoft Edge	Локальный	DoS	2024-08-23	✓
7	Высокая	CVE-2024-7972	Microsoft Edge	Сетевой	OSI	2024-08-23	✓
8	Высокая	CVE-2024-7971	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
9	Высокая	CVE-2024-7965	Microsoft Edge	Сетевой	OSI	2024-08-23	✓
10	Высокая	CVE-2024-7967	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
11	Высокая	CVE-2024-7974	Microsoft Edge	Сетевой	OSI	2024-08-23	✓

12	Высокая	CVE-2024-38209	Microsoft Edge	Локальный	DoS	2024-08-23	✓
13	Высокая	CVE-2024-7973	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
14	Критическая	CVE-2024-28000	LiteSpeed Technologies LiteSpeed Cache plugin for WordPress	Сетевой	PE	2024-08-23	✓
15	Высокая	CVE-2024-7980	Microsoft Edge	Локальный	OSI	2024-08-23	✓
16	Высокая	CVE-2024-7964	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
17	Высокая	CVE-2024-7968	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
18	Высокая	CVE-2024-7966	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
19	Высокая	CVE-2024-7969	Microsoft Edge	Сетевой	ACE	2024-08-23	✓
20	Высокая	CVE-2024-7979	Microsoft Edge	Локальный	OSI	2024-08-23	✓
21	Высокая	CVE-2024-7987	Rockwell Automation ThinManager and ThinServer	Локальный	PE	2024-08-23	✓
22	Критическая	CVE-2024-7988	Rockwell Automation ThinManager and ThinServer	Сетевой	WLF	2024-08-23	✓
23	Высокая	CVE-2024-43689	ELECOM wireless LAN routers and access points	Смежная сеть	ACE	2024-08-27	✓
24	Высокая	CVE-2024-39300	ELECOM wireless LAN routers and access points	Сетевой	OSI	2024-08-27	✓
25	Высокая	CVE-2024-6456	AVEVA Historian Web Server	Сетевой	ACE	2024-08-22	✓

26	Критическая	CVE-2024-6078	Rockwell Automation DataMosaix Private Cloud	Сетевой	SB	2024-08-22	✓
27	Высокая	CVE-2024-7965	Google Chrome	Сетевой	OSI	2024-08-22	✓
28	Высокая	CVE-2024-7966	Google Chrome	Сетевой	ACE	2024-08-22	✓
29	Высокая	CVE-2024-7967	Google Chrome	Сетевой	ACE	2024-08-22	✓
30	Высокая	CVE-2024-7968	Google Chrome	Сетевой	ACE	2024-08-22	✓
31	Высокая	CVE-2024-7969	Google Chrome	Сетевой	ACE	2024-08-22	✓
32	Высокая	CVE-2024-7971	Google Chrome	Сетевой	ACE	2024-08-22	✓
33	Высокая	CVE-2024-7972	Google Chrome	Сетевой	OSI	2024-08-22	✓
34	Высокая	CVE-2024-7973	Google Chrome	Сетевой	ACE	2024-08-22	✓
35	Высокая	CVE-2024-7974	Google Chrome	Сетевой	OSI	2024-08-22	✓
36	Высокая	CVE-2024-7964	Google Chrome	Сетевой	ACE	2024-08-22	✓
37	Высокая	CVE-2024-7977	Google Chrome	Локальный	OSI	2024-08-22	✓
38	Высокая	CVE-2024-7979	Google Chrome	Локальный	OSI	2024-08-22	✓
39	Высокая	CVE-2024-7980	Google Chrome	Локальный	OSI	2024-08-22	✓
40	Высокая	CVE-2024-20375	Cisco Unified Communications Manager	Сетевой	DoS	2024-08-21	✓

41	Высокая	CVE-2024-7305	Autodesk AutoCAD products	Локальный	ACE	2024-08-21	✓
42	Высокая	CVE-2024-7352	PDF-XChange Editor	Сетевой	ACE	2024-08-21	✓
43	Критическая	CVE-2024-22252	Dell PowerFlex Appliance	Локальный	ACE	2024-08-21	✓
44	Критическая	CVE-2024-22253	Dell PowerFlex Appliance	Локальный	ACE	2024-08-21	✓
45	Высокая	CVE-2024-22254	Dell PowerFlex Appliance	Локальный	OSI	2024-08-21	✓
46	Высокая	CVE-2024-6788	Phoenix Contact CHARX controllers	Сетевой	OSI	2024-08-21	✓
47	Высокая	CVE-2024-3913	Phoenix Contact CHARX controllers	Сетевой	OSI	2024-08-21	✓
48	Критическая	CVE-2024-43440	Moodle	Сетевой	ACE	2024-08-20	✓
49	Высокая	CVE-2024-43432	Moodle	Сетевой	OSI	2024-08-20	✓
50	Высокая	CVE-2024-43428	Moodle	Сетевой	OSI	2024-08-20	✓
51	Высокая	CVE-2024-43427	Moodle	Сетевой	OSI	2024-08-20	✓
52	Высокая	CVE-2024-43426	Moodle	Сетевой	OSI	2024-08-20	✓
53	Высокая	CVE-2024-43425	Moodle	Сетевой	ACE	2024-08-20	✓
54	Высокая	CVE-2024-30188	Apache DolphinScheduler	Сетевой	PE	2024-08-20	✓
55	Критическая	CVE-2024-43202	Apache DolphinScheduler	Сетевой	ACE	2024-08-20	✓

56	Высокая	CVE-2024-7399	Samsung MagicINFO 9 Server	Сетевой	RLF	2024-08-19	✓
57	Высокая	CVE-2024-43374	Vim	Сетевой	ACE	2024-08-15	✓
58	Высокая	CVE-2024-7272	FFmpeg	Сетевой	ACE	2024-08-15	✓
59	Критическая	CVE-2024-5914	Palo Alto Networks Cortex XSOAR CommonScripts Pack	Сетевой	ACE	2024-08-14	✓
60	Высокая	CVE-2024-30045	Siemens INTRALOG WMS	Сетевой	ACE	2024-08-14	✓
61	Высокая	CVE-2024-0056	Siemens INTRALOG WMS	Сетевой	OSI	2024-08-14	✓
62	Высокая	CVE-2024-32636	Siemens Teamcenter Visualization and JT2Go	Локальный	OSI	2024-08-14	✓
63	Высокая	CVE-2024-32635	Siemens Teamcenter Visualization and JT2Go	Локальный	OSI	2024-08-14	✓
64	Критическая	CVE-2024-42367	aiohttp	Сетевой	OSI	2024-08-14	✓
65	Высокая	CVE-2024-41908	Siemens NX	Локальный	ACE	2024-08-14	✓
66	Высокая	CVE-2024-38171	Microsoft PowerPoint	Локальный	ACE	2024-08-14	✓
67	Критическая	CVE-2024-38109	Microsoft Azure Health Bot	Сетевой	CSRF	2024-08-14	✓
68	Высокая	CVE-2024-39388	Adobe Substance 3D Stager	Локальный	ACE	2024-08-13	✓
69	Высокая	CVE-2024-41864	Adobe Substance 3D Designer	Локальный	ACE	2024-08-13	✓

70	Высокая	CVE-2024-34117	Adobe Photoshop	Локальный	ACE	2024-08-13	✓
71	Высокая	CVE-2024-41858	Adobe InCopy	Локальный	ACE	2024-08-13	✓
72	Критическая	CVE-2024-7593	Ivanti Virtual Traffic Manager	Сетевой	OSI	2024-08-14	✓

1

Краткое описание: Отказ в обслуживании в Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix and Compact GuardLogix 5380

Идентификатор уязвимости: CVE-2024-40619

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

Уязвимый продукт: ControlLogix 5580: 34.011
GuardLogix 5580: 34.011

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-26 / 2024-08-26

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD%201690.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-226-03

2

Краткое описание: Отказ в обслуживании в Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix and Compact GuardLogix 5380

Идентификатор уязвимости: CVE-2024-7515

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: CompactLogix 5380: до 36.011
CompactLogix 5480: до 36.011
ControlLogix 5580: до 36.011
GuardLogix 5580: до 36.011
Compact GuardLogix 5380: до 36.011

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-26 / 2024-08-26

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD%201686.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-226-10

3

Краткое описание: Отказ в обслуживании в Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix and Compact GuardLogix 5380

Идентификатор уязвимости: CVE-2024-7507

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: CompactLogix 5380: до 36.011
CompactLogix 5480: до 36.011
ControlLogix 5580: до 36.011
GuardLogix 5580: до 36.011
Compact GuardLogix 5380: до 36.011

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-26 / 2024-08-26

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD%201685.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-226-09

4

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7977

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7977

5

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-41879

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-41879

6

Краткое описание: Отказ в обслуживании в Microsoft Edge

Идентификатор уязвимости: CVE-2024-38210

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft 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: 7.8 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38210

7

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7972

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7972

8

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7971

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7971

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7965

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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: 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7965

10

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7967

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7967

11

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7974

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7974

12

Краткое описание: Отказ в обслуживании в Microsoft Edge

Идентификатор уязвимости: CVE-2024-38209

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft 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: 7.8 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-38209

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7973

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7973

14

Краткое описание: Повышение привилегий в LiteSpeed Technologies LiteSpeed Cache plugin for WordPress

Идентификатор уязвимости: CVE-2024-28000

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: LiteSpeed Cache: 1.0.15 - 6.3.0.1

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-6-3-0-1-unauthenticated-privilege-escalation-vulnerability?_s_id=cve
- http://patchstack.com/articles/critical-privilege-escalation-in-litespeed-cache-plugin-affecting-5-million-sites?_s_id=cve

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7980

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7980

16

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7964

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7964

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7968

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7968

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7966

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7966

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7969

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

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7969

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2024-7979

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 127.0.2651.105

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

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: 7.8 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: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-7979

Краткое описание: Повышение привилегий в Rockwell Automation ThinManager and ThinServer

Идентификатор уязвимости: CVE-2024-7987

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: ThinManager: 11.1.0 - 13.2.1
ThinServer: 11.1.0 - 13.2.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://www.rockwellautomation.com/en-ca/trust-center/security-advisories/advisory.SD1692.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1157/

Краткое описание: Запись локальных файлов в Rockwell Automation ThinManager and ThinServer

Идентификатор уязвимости: CVE-2024-7988

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: ThinManager: 11.1.0 - 13.2.1
ThinServer: 11.1.0 - 13.2.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-23 / 2024-08-23

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1158/
- http://www.rockwellautomation.com/en-ca/trust-center/security-advisories/advisory.SD1692.html

Краткое описание: Выполнение произвольного кода в ELECOM wireless LAN routers and access points

Идентификатор уязвимости: CVE-2024-43689

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: WAB-I1750-PS: 1.5.10
WAB-S1167-PS: 1.5.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-27 / 2024-08-27

Ссылки на источник:

- http://jvn.jp/en/jp/JVN24885537/index.html
- http://www.elecom.co.jp/news/security/20240827-01/

24

Краткое описание: Получение конфиденциальной информации в ELECOM wireless LAN routers and access points

Идентификатор уязвимости: CVE-2024-39300

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: WAB-I1750-PS: 1.5.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-27 / 2024-08-27

Ссылки на источник:

- http://jvn.jp/en/jp/JVN24885537/index.html
- http://www.elecom.co.jp/news/security/20240827-01/

Краткое описание: Выполнение произвольного кода в AVEVA Historian Web Server

Идентификатор уязвимости: CVE-2024-6456

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

Уязвимый продукт: Historian Server: 2020 R2 SP1 P01 - 2023 R2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

25

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

Оценка CVSSv3: 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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-228-10

26

Краткое описание: Обход безопасности в Rockwell Automation DataMosaix Private Cloud

Идентификатор уязвимости: CVE-2024-6078

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: DataMosaix Private Cloud: до 7.09

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD%201687.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-226-05

27

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7965

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/356196918

28

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7966

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/355465305

29

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7967

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/355731798

30

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7968

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/349253666

31

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7969

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/351865302

32

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7971

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/360700873

33

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7972

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/345960102

34

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7973

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/345518608

35

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7974

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/339141099

36

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7964

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/358296941

37

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7977

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/324770940

38

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7979

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/356064205

39

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7980

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 127.0.6533.120

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: 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: 2024-08-22 / 2024-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- http://crbug.com/356328460

40

Краткое описание: Отказ в обслуживании в Cisco Unified Communications Manager

Идентификатор уязвимости: CVE-2024-20375
BDU:2024-06406

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Cisco Unified Communications Manager: до 15SU1

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-dos-kkHq43We
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwi68892
- https://bdu.fstec.ru/vul/2024-06406

41

Краткое описание: Выполнение произвольного кода в Autodesk AutoCAD products

Идентификатор уязвимости: CVE-2024-7305
BDU:2024-06373

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk AutoCAD: 2025
AutoCAD Architecture: 2025
AutoCAD Electrical: 2025
AutoCAD Mechanical: 2025
AutoCAD MEP: 2025
AutoCAD Plant 3D: 2025
Autodesk Civil 3D: 2025
Advance Steel: 2025
AutoCAD LT: 2025
DWG Trueview: 2025

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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0014
- http://www.zerodayinitiative.com/advisories/ZDI-24-1153/
- https://bdu.fstec.ru/vul/2024-06373

Краткое описание: Выполнение произвольного кода в PDF-XChange Editor

Идентификатор уязвимости: CVE-2024-7352

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PDF-XChange Editor: до 10.3.0.386

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR: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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-24-1037/

43

Краткое описание: Выполнение произвольного кода в Dell PowerFlex Appliance

Идентификатор уязвимости: CVE-2024-22252
BDU:2024-01807

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PowerFlex Appliance: до IC-46.380.01

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225976/dsa-2024-245-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01807

44

Краткое описание: Выполнение произвольного кода в Dell PowerFlex Appliance

Идентификатор уязвимости: CVE-2024-22253
BDU:2024-01808

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PowerFlex Appliance: до IC-46.380.01

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225976/dsa-2024-245-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01808

45

Краткое описание: Получение конфиденциальной информации в Dell PowerFlex Appliance

Идентификатор уязвимости: CVE-2024-22254
BDU:2024-01810

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PowerFlex Appliance: до IC-46.380.01

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000225976/dsa-2024-245-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities
- https://bdu.fstec.ru/vul/2024-01810

Краткое описание: Получение конфиденциальной информации в Phoenix Contact CHARX controllers

Идентификатор уязвимости: CVE-2024-6788

Идентификатор программной ошибки: CWE-1188 Инициализация ресурса с небезопасными параметрами по умолчанию

Уязвимый продукт: CHARX SEC-3000: до 1.6.3
CHARX SEC-3050: до 1.6.3
CHARX SEC-3100: до 1.6.3
CHARX SEC-3150: до 1.6.3

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

46 **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: 8.6 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://cert.vde.com/en/advisories/VDE-2024-022

47

Краткое описание: Получение конфиденциальной информации в Phoenix Contact CHARX controllers

Идентификатор уязвимости: CVE-2024-3913

Идентификатор программной ошибки: CWE-552 Непредусмотренный доступ к файлам или каталогам

Уязвимый продукт: CHARX SEC-3100: до 1.6.3
CHARX SEC-3000: до 1.6.3
CHARX SEC-3050: до 1.6.3
CHARX SEC-3150: до 1.6.3

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2024-08-21 / 2024-08-21

Ссылки на источник:

- http://cert.vde.com/en/advisories/VDE-2024-022
- http://www.zerodayinitiative.com/advisories/ZDI-24-1152/

Краткое описание: Выполнение произвольного кода в Moodle

Идентификатор уязвимости: CVE-2024-43440

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Moodle: 4.1.0 - 4.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=461210

Краткое описание: Получение конфиденциальной информации в Moodle

Идентификатор уязвимости: CVE-2024-43432

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

Уязвимый продукт: Moodle: 4.1.0 - 4.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=461200

Краткое описание: Получение конфиденциальной информации в Moodle

Идентификатор уязвимости: CVE-2024-43428

Идентификатор программной ошибки: CWE-524 Разглашение информации, связанное с кэшированием

Уязвимый продукт: Moodle: 4.1.0 - 4.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=461196

Краткое описание: Получение конфиденциальной информации в Moodle

Идентификатор уязвимости: CVE-2024-43427

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

Уязвимый продукт: Moodle: 4.1.0 - 4.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=461195

Краткое описание: Получение конфиденциальной информации в Moodle

Идентификатор уязвимости: CVE-2024-43426

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

Уязвимый продукт: Moodle: 4.1.0 - 4.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=461194

53

Краткое описание: Выполнение произвольного кода в Moodle

Идентификатор уязвимости: CVE-2024-43425

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Moodle: 4.1.0 - 4.4.1

Категория уязвимого продукта: Прикладное программное обеспечение

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.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://moodle.org/mod/forum/discuss.php?d=461193

54

Краткое описание: Повышение привилегий в Apache DolphinScheduler

Идентификатор уязвимости: CVE-2024-30188

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

Уязвимый продукт: DolphinScheduler: 3.0.0 - 3.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://lists.apache.org/thread/tbrt42mnr42bq6scxwt6bjr3s2pwyd07
- http://lists.apache.org/thread/q190csod90nk667zss3ycg8z2tmxhzfc

55

Краткое описание: Выполнение произвольного кода в Apache DolphinScheduler

Идентификатор уязвимости: CVE-2024-43202

Идентификатор программной ошибки: CWE-676 Использование потенциально опасной функции

Уязвимый продукт: DolphinScheduler: 3.0.0 - 3.2.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-20 / 2024-08-20

Ссылки на источник:

- http://lists.apache.org/thread/8jxnnkrkl2st2kd37ng123lobcky7cfj
- http://github.com/apache/dolphinscheduler/pull/15758

56

Краткое описание: Чтение локальных файлов в Samsung MagicINFO 9 Server

Идентификатор уязвимости: CVE-2024-7399

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

Уязвимый продукт: MagicINFO 9 Server: до 21.1050

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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: 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: 2024-08-19 / 2024-08-19

Ссылки на источник:

- http://security.samsungtv.com/securityUpdates
- http://www.zerodayinitiative.com/advisories/ZDI-24-1128/

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2024-43374

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Vim: 9.1.0 - 9.1.0677

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-15 / 2024-08-15

Ссылки на источник:

- http://github.com/vim/vim/security/advisories/GHSA-2w8m-443v-cgvw

58

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2024-7272
BDU:2024-06374

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

Уязвимый продукт: FFmpeg: 5.0 - 5.1.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-15 / 2024-08-15

Ссылки на источник:

- http://vuldb.com/?id.273945
- http://vuldb.com/?ctiid.273945
- http://github.com/CookedMelon/ReportCVE/tree/main/FFmpeg/poc5
- http://github.com/CookedMelon/ReportCVE/tree/main/FFmpeg/poc6
- https://bdu.fstec.ru/vul/2024-06374

Краткое описание: Выполнение произвольного кода в Palo Alto Networks Cortex XSOAR CommonScripts Pack

Идентификатор уязвимости: CVE-2024-5914

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

Уязвимый продукт: Cortex XSOAR CommonScripts: до 1.12.33

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://security.paloaltonetworks.com/CVE-2024-5914

Краткое описание: Выполнение произвольного кода в Siemens INTRALOG WMS

Идентификатор уязвимости: CVE-2024-30045
BDU:2024-03969

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

Уязвимый продукт: INTRALOG WMS: до 4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-417547.txt
- https://bdu.fstec.ru/vul/2024-03969

Краткое описание: Получение конфиденциальной информации в Siemens INTRALOG WMS

Идентификатор уязвимости: CVE-2024-0056
BDU:2024-00281

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: INTRALOG WMS: до 4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.7 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-417547.txt
- https://bdu.fstec.ru/vul/2024-00281

Краткое описание: Получение конфиденциальной информации в Siemens Teamcenter Visualization and JT2Go

Идентификатор уязвимости: CVE-2024-32636
BDU:2024-04964

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Teamcenter Visualization: до 2312.0005
JT2Go: до 2312.0005

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

62

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-856475.txt
- https://bdu.fstec.ru/vul/2024-04964

Краткое описание: Получение конфиденциальной информации в Siemens Teamcenter Visualization and JT2Go

Идентификатор уязвимости: CVE-2024-32635

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Teamcenter Visualization: до 2312.0005
JT2Go: до 2312.0005

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

63

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/txt/ssa-856475.txt

64

Краткое описание: Получение конфиденциальной информации в aiohttp

Идентификатор уязвимости: CVE-2024-42367

Идентификатор программной ошибки: CWE-61 Уязвимости, связанные с символическими ссылками UNIX

Уязвимый продукт: aiohttp: 3.0.0 - 3.10.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка 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: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://github.com/aio-libs/aiohttp/security/advisories/GHSA-jwhx-xcg6-8xhj
- http://github.com/aio-libs/aiohttp/pull/8653
- http://github.com/aio-libs/aiohttp/commit/ce2e9758814527589b10759a20783fb03b98339f
- http://github.com/aio-libs/aiohttp/blob/e0ff5246e1d29b7710ab1a2bbc972b48169f1c05/aiohttp/web_fileresponse.py#L177
- http://github.com/aio-libs/aiohttp/blob/e0ff5246e1d29b7710ab1a2bbc972b48169f1c05/aiohttp/web_urldispatcher.py#L674

Краткое описание: Выполнение произвольного кода в Siemens NX

Идентификатор уязвимости: CVE-2024-41908

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: NX: до 2406.3000

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-357412.html

66

Краткое описание: Выполнение произвольного кода в Microsoft PowerPoint

Идентификатор уязвимости: CVE-2024-38171

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Microsoft PowerPoint: 2016
Microsoft Office LTSC 2021: 32 bit editions - 2021 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171
- http://www.zerodayinitiative.com/advisories/ZDI-24-1148/

67

Краткое описание: Подделка запросов на стороне сервера в Microsoft Azure Health Bot

Идентификатор уязвимости: CVE-2024-38109

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

Уязвимый продукт: Azure Health Bot: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Подделка запросов на стороне сервера

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38109

68

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

Идентификатор уязвимости: CVE-2024-39388

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Stager: 2.0.0 - 3.0.2

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb24-60.html
- http://www.zerodayinitiative.com/advisories/ZDI-24-1144/

69

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

Идентификатор уязвимости: CVE-2024-41864

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: 10.1.0 - 13.1.2

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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_designer/apsb24-67.html

70

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2024-34117

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Photoshop: 20.0 - 25.9.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb24-49.html

Краткое описание: Выполнение произвольного кода в Adobe InCopy

Идентификатор уязвимости: CVE-2024-41858

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

Уязвимый продукт: InCopy: 15.0.0 - 19.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

71 **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: 2024-08-13 / 2024-08-13

Ссылки на источник:

- http://helpx.adobe.com/security/products/incopy/apsb24-64.html

Краткое описание: Получение конфиденциальной информации в Ivanti Virtual Traffic Manager

Идентификатор уязвимости: CVE-2024-7593
BDU:2024-06372

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: Virtual Traffic Manager: 22.2 - 22.7R1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

72 **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: 2024-08-14 / 2024-08-14

Ссылки на источник:

- http://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593
- https://bdu.fstec.ru/vul/2024-06372