НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-07-29.1 | 29 июля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-3651	Dell SmartFabric OS10	Сетевой	DoS	2024-07-29	✓
2	Критическая	CVE-2024-2961	Dell SmartFabric OS10	Сетевой	ACE	2024-07-29	✓
3	Высокая	CVE-2024-32230	FFmpeg	Сетевой	ACE	2024-07-22	✓
4	Высокая	CVE-2024-5602	National Instruments I/O TRACE	Локальный	ACE	2024-07-25	✓
5	Высокая	CVE-2024-4081	National Instruments LabVIEW	Локальный	ACE	2024-07-25	✓
6	Высокая	CVE-2024-4080	National Instruments LabVIEW	Локальный	ACE	2024-07-25	✓
7	Высокая	CVE-2024-4079	National Instruments LabVIEW	Локальный	OSI	2024-07-25	✓
8	Критическая	CVE-2024-37998	Siemens SICAM Products	Сетевой	OSI	2024-07-25	✓
9	Высокая	CVE-2024-6387	Bosch PRC7000	Сетевой	ACE	2024-07-26	✓
10	Высокая	CVE-2024-36971	Google ChromeOS	Локальный	PE	2024-07-26	✓
11	Высокая	CVE-2024-6100	Google ChromeOS	Сетевой	ACE	2024-07-26	✓
12	Высокая	CVE-2024-5497	Google ChromeOS	Сетевой	ACE	2024-07-26	✓
13	Высокая	CVE-2024-7001	Google Chrome	Сетевой	OSI	2024-07-24	✓

14	Высокая	CVE-2024-7000	Google Chrome	Сетевой	ACE	2024-07-24	✓
15	Высокая	CVE-2024-6998	Google Chrome	Сетевой	ACE	2024-07-24	✓
16	Высокая	CVE-2024-6997	Google Chrome	Сетевой	ACE	2024-07-24	✓
17	Высокая	CVE-2024-6996	Google Chrome	Сетевой	ACE	2024-07-24	✓
18	Высокая	CVE-2024-6994	Google Chrome	Сетевой	ACE	2024-07-24	✓
19	Высокая	CVE-2024-6993	Google Chrome	Сетевой	OSI	2024-07-24	✓
20	Высокая	CVE-2024-6992	Google Chrome	Сетевой	ACE	2024-07-24	✓
21	Высокая	CVE-2024-6991	Google Chrome	Сетевой	ACE	2024-07-24	✓
22	Высокая	CVE-2024-6989	Google Chrome	Сетевой	ACE	2024-07-24	✓
23	Высокая	CVE-2024-6988	Google Chrome	Сетевой	ACE	2024-07-24	✓
24	Высокая	CVE-2024-38176	Microsoft GroupMe	Сетевой	OSI	2024-07-26	✓
25	Критическая	CVE-2024-38164	Microsoft GroupMe	Сетевой	PE	2024-07-26	✓
26	Критическая	CVE-2024-5217	ServiceNow	Сетевой	ACE	2024-07-26	✓
27	Критическая	CVE-2024-4879	ServiceNow	Сетевой	ACE	2024-07-26	✓
28	Высокая	CVE-2024-39540	Juniper Junos OS	Сетевой	DoS	2024-07-22	✓

29	Высокая	CVE-2024-1575	Zyxel in APs	Сетевой	OSI	2024-07-23	✓

1

Краткое описание: Отказ в обслуживании в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2024-3651
BDU:2024-04211

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

Уязвимый продукт: SmartFabric OS10: 10.5.5.9

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2024-07-29 / 2024-07-29

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000226956/dsa-2024-315-security-update-for-dell-os10-third-party-vulnerabilities
- https://bdu.fstec.ru/vul/2024-04211

2

Краткое описание: Выполнение произвольного кода в Dell SmartFabric OS10

Идентификатор уязвимости: CVE-2024-2961
BDU:2024-03171

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

Уязвимый продукт: SmartFabric OS10: 10.5.5.9

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:P/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-29 / 2024-07-29

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000226956/dsa-2024-315-security-update-for-dell-os10-third-party-vulnerabilities
- https://bdu.fstec.ru/vul/2024-03171

3

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2024-32230

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

Уязвимый продукт: FFmpeg: до 7.0.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-22 / 2024-07-22

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10952

4

Краткое описание: Выполнение произвольного кода в National Instruments I/O TRACE

Идентификатор уязвимости: CVE-2024-5602

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: I/O TRACE: 24.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера

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: 2024-07-25 / 2024-07-25

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/stack-based-buffer-overflow-vulnerability-in-ni-io-trace-tool.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-205-01

5

Краткое описание: Выполнение произвольного кода в National Instruments LabVIEW

Идентификатор уязвимости: CVE-2024-4081

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

Уязвимый продукт: LabVIEW: 2020 - 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-07-25 / 2024-07-25

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/memory-corruption-issues-due-to-improper-length-checks-in-labview.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-205-03

6

Краткое описание: Выполнение произвольного кода в National Instruments LabVIEW

Идентификатор уязвимости: CVE-2024-4080

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

Уязвимый продукт: LabVIEW: 2020 - 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2024-07-25 / 2024-07-25

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/memory-corruption-issues-due-to-improper-length-checks-in-labview.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-205-03

7

Краткое описание: Получение конфиденциальной информации в National Instruments LabVIEW

Идентификатор уязвимости: CVE-2024-4079

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: LabVIEW: 2020 - 2024 Q1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-25 / 2024-07-25

Ссылки на источник:

- http://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/out-of-bounds-read-due-to-missing-bounds-check-in-labview.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-205-03

Краткое описание: Получение конфиденциальной информации в Siemens SICAM Products

Идентификатор уязвимости: CVE-2024-37998
BDU:2024-05672

Идентификатор программной ошибки: CWE-620 Смена пароля без подтверждения

Уязвимый продукт: SICAM A8000: все версии
SICAM 8: все версии
SICAM EGS: все версии
CPCI85 Central Processing/Communication: до 5.40
SICORE Base system: до 1.4.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход ограничений безопасности

8

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-25 / 2024-07-25

Ссылки на источник:

- http://cert-portal.siemens.com/productcert/html/ssa-071402.html
- https://bdu.fstec.ru/vul/2024-05672

Краткое описание: Выполнение произвольного кода в Bosch PRC7000

Идентификатор уязвимости: CVE-2024-6387
BDU:2024-04914

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

Уязвимый продукт: PRC7000: 1.11.12.4 - 1.11.13.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

9

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://psirt.bosch.com/security-advisories/bosch-sa-258444.html
- https://bdu.fstec.ru/vul/2024-04914

Краткое описание: Повышение привилегий в Google ChromeOS

Идентификатор уязвимости: CVE-2024-36971
BDU:2024-04585

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 120.0.6099.318

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

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/long-term-support-channel-update-for_25.html
- https://bdu.fstec.ru/vul/2024-04585

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-6100
BDU:2024-04870

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

Уязвимый продукт: Chrome OS: до 120.0.6099.318

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/long-term-support-channel-update-for_25.html
- https://bdu.fstec.ru/vul/2024-04870

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-5497
BDU:2024-04338

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

Уязвимый продукт: Chrome OS: до 120.0.6099.318

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/long-term-support-channel-update-for_25.html
- https://bdu.fstec.ru/vul/2024-04338

13

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7001

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/347509736

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7000

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/339877158

15

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6998

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/340098902

16

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6997

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/325293263

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6996

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

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/333708039

18

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6994

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

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/339686368

19

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-6993

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/349903568

20

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6992

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/349653220

21

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6991

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/346618785

22

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6989

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/349342289

23

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6988

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 107.0.5304.89 - 127.0.6533.57

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-24 / 2024-07-24

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/07/stable-channel-update-for-desktop_23.html
- http://issues.chromium.org/issues/349198731

Краткое описание: Получение конфиденциальной информации в Microsoft GroupMe

Идентификатор уязвимости: CVE-2024-38176

Идентификатор программной ошибки: CWE-307 Некорректное ограничение количества неудачных попыток аутентификации

Уязвимый продукт: GroupMe: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38176

Краткое описание: Повышение привилегий в Microsoft GroupMe

Идентификатор уязвимости: CVE-2024-38164

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: GroupMe: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38164

26

Краткое описание: Выполнение произвольного кода в ServiceNow

Идентификатор уязвимости: CVE-2024-5217

Идентификатор программной ошибки: CWE-184 Неполный черный список

Уязвимый продукт: ServiceNow: до Washington DC Patch 5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313
- http://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1644293

27

Краткое описание: Выполнение произвольного кода в ServiceNow

Идентификатор уязвимости: CVE-2024-4879

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ServiceNow: до Washington DC Patch 4

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-07-26 / 2024-07-26

Ссылки на источник:

- http://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154
- http://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1644293

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2024-39540

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

Уязвимый продукт: Juniper Junos OS: 21.2R3-S5

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 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: 2024-07-22 / 2024-07-22

Ссылки на источник:

- http://supportportal.juniper.net/JSA83000

29

Краткое описание: Получение конфиденциальной информации в Zyxel in APs

Идентификатор уязвимости: CVE-2024-1575

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: NWA50AX: 6.29(ABYW.4)
NWA50AX-PRO: 6.65(ACGE.1)
NWA55AXE: 6.29(ABZL.4)
NWA90AX: 6.29(ACCV.4)
NWA90AX-PRO: 6.65(ACGF.1)
NWA110AX: 6.70(ABTG.2)
NWA210AX: 6.70(ABTD.2)
NWA220AX-6E: 6.70(ACCO.1)
NWA1123ACv3: 6.70(ABVT.1)
WAC500: 6.70(ABVS.1)
WAC500H: 6.70(ABWA.1)
WAX300H: 6.70(ACHF.1)
WAX510D: 6.70(ABTF.2)
WAX610D: 6.70(ABTE.2)
WAX620D-6E: 6.70(ACCN.1)
WAX630S: 6.70(ABZD.2)
WAX640S-6E: 6.70(ACCM.1)
WAX650S: 6.70(ABRM.2)
WAX655E: 6.70(ACDO.1)
WBE660S: 6.70(ACGG.2)

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: 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: 2024-07-23 / 2024-07-23

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-improper-privilege-management-vulnerability-in-aps-07-23-2024