НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-04-03.1 | 3 апреля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-48022	Anyscale Ray	Сетевой	ACE	2024-03-29	✓
2	Критическая	CVE-2023-48023	Anyscale Ray	Сетевой	CSRF	2024-03-29	✓
3	Высокая	CVE-2023-6021	Anyscale Ray	Сетевой	RLF	2024-03-29	✓
4	Высокая	CVE-2023-6020	Anyscale Ray	Сетевой	RLF	2024-03-29	✓
5	Критическая	CVE-2023-6019	Anyscale Ray	Сетевой	ACE	2024-03-29	✓
6	Высокая	CVE-2024-2929	Rockwell Automation Arena Simulation	Локальный	ACE	2024-03-27	✓
7	Высокая	CVE-2024-21919	Rockwell Automation Arena Simulation	Локальный	ACE	2024-03-27	✓
8	Высокая	CVE-2024-20259	Cisco IOS XE Software	Сетевой	DoS	2024-03-28	✓
9	Высокая	CVE-2024-20271	Cisco Access Point Software	Сетевой	DoS	2024-03-28	✓
10	Высокая	CVE-2024-21918	Rockwell Automation Arena Simulation	Локальный	ACE	2024-03-27	✓
11	Высокая	CVE-2024-20308	Cisco IOS and IOS XE Software	Сетевой	DoS	2024-03-28	✓
12	Высокая	CVE-2024-21913	Rockwell Automation Arena Simulation	Локальный	ACE	2024-03-27	✓
13	Высокая	CVE-2024-21912	Rockwell Automation Arena Simulation	Локальный	ACE	2024-03-27	✓

14	Высокая	CVE-2024-2887	Google Chrome	Сетевой	ACE	2024-03-27	✓
15	Высокая	CVE-2024-2886	Google Chrome	Сетевой	ACE	2024-03-27	✓
16	Высокая	CVE-2024-2885	Google Chrome	Сетевой	ACE	2024-03-27	✓
17	Высокая	CVE-2024-2883	Google Chrome	Сетевой	ACE	2024-03-27	✓
18	Высокая	CVE-2024-30204	GNU Emacs	Сетевой	ACE	2024-03-26	✓
19	Высокая	CVE-2024-30203	GNU Emacs	Сетевой	ACE	2024-03-26	✓
20	Высокая	CVE-2024-30202	GNU Emacs	Сетевой	ACE	2024-03-26	✓
21	Высокая	CVE-2024-30205	GNU Emacs	Сетевой	OSI	2024-03-26	✓
22	Высокая	CVE-2024-1753	Podman	Локальный	PE	2024-03-26	✓
23	Высокая	CVE-2024-1580	macOS Sonoma, macOS Ventura и Apple Safari	Сетевой	ACE	2024-03-26	✓

1

Краткое описание: Выполнение произвольного кода в Anyscale Ray

Идентификатор уязвимости: CVE-2023-48022

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Anyscale Ray: версии 2.6.3 и 2.8.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-29 / 2024-03-29

Ссылки на источник:

- http://bishopfox.com/blog/ray-versions-2-6-3-2-8-0
- http://www.anyscale.com/blog/update-on-ray-cves-cve-2023-6019-cve-2023-6020-cve-2023-6021-cve-2023-48022-cve-2023-48023

2

Краткое описание: Подделка запросов на стороне сервера в Anyscale Ray

Идентификатор уязвимости: CVE-2023-48023

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

Уязвимый продукт: Anyscale Ray: версии 2.6.3 и 2.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

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:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-29 / 2024-03-29

Ссылки на источник:

- http://bishopfox.com/blog/ray-versions-2-6-3-2-8-0
- http://www.anyscale.com/blog/update-on-ray-cves-cve-2023-6019-cve-2023-6020-cve-2023-6021-cve-2023-48022-cve-2023-48023

3

Краткое описание: Чтение локальных файлов в Anyscale Ray

Идентификатор уязвимости: CVE-2023-6021

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

Уязвимый продукт: Anyscale Ray: с версии 0.1.0 по 2.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-29 / 2024-03-29

Ссылки на источник:

- http://huntr.com/bounties/5039c045-f986-4cbc-81ac-370fe4b0d3f8
- http://www.anyscale.com/blog/update-on-ray-cves-cve-2023-6019-cve-2023-6020-cve-2023-6021-cve-2023-48022-cve-2023-48023

4

Краткое описание: Чтение локальных файлов в Anyscale Ray

Идентификатор уязвимости: CVE-2023-6020

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

Уязвимый продукт: Anyscale Ray: с версии 0.1.0 по 2.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-29 / 2024-03-29

Ссылки на источник:

- http://huntr.com/bounties/83dd8619-6dc3-4c98-8f1b-e620fedcd1f6
- http://www.anyscale.com/blog/update-on-ray-cves-cve-2023-6019-cve-2023-6020-cve-2023-6021-cve-2023-48022-cve-2023-48023

Краткое описание: Выполнение произвольного кода в Anyscale Ray

Идентификатор уязвимости: CVE-2023-6019

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

Уязвимый продукт: Anyscale Ray: с версии 0.1.0 по 2.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

5

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-29 / 2024-03-29

Ссылки на источник:

- http://huntr.com/bounties/d0290f3c-b302-4161-89f2-c13bb28b4cfe
- http://www.anyscale.com/blog/update-on-ray-cves-cve-2023-6019-cve-2023-6020-cve-2023-6021-cve-2023-48022-cve-2023-48023

6

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena Simulation

Идентификатор уязвимости: CVE-2024-2929

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

Уязвимый продукт: Arena Simulation Software: 16.00

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/support/advisory.SD-1665.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03

7

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena Simulation

Идентификатор уязвимости: CVE-2024-21919

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Arena Simulation Software: 16.00

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/support/advisory.SD-1665.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03

8

Краткое описание: Отказ в обслуживании в Cisco IOS XE Software

Идентификатор уязвимости: CVE-2024-20259

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

Уязвимый продукт: Cisco IOS XE: с версии 17.9.3 по 17.9.4a

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-28 / 2024-03-28

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dhcp-dos-T3CXPO9z
- https://bdu.fstec.ru/vul/2024-02370

9

Краткое описание: Отказ в обслуживании в Cisco Access Point Software

Идентификатор уязвимости: CVE-2024-20271

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: 6300 Series Embedded Services Access Points: все версии
Cisco Aironet 1540 Series Access Points: все версии
Aironet 1560 Series Access Points: все версии
Aironet 1800 Series Access Points: все версии
Aironet 2800 Series Access Points: все версии
Aironet 3800 Series Access Points: все версии
Aironet 4800 Access Points: все версии
Business 100 Series Mesh Extenders: все версии
Business 200 Series Access Points: все версии
Catalyst 9100 Access Points: все версии
Catalyst IW6300 Heavy Duty Series Access Points: все версии
Integrated Access Point on 1100 Integrated Services Routers: все версии
Wide Pluggable Form Factor Wi-Fi 6 AP Module for Industrial Routers: все версии
Wireless LAN Controller Software: 8.9 - 8.10
Catalyst 9800 Wireless Controller Software: 17.2 - 17.12
Business Wireless Access Point Software: 10.5.2 - 10.9.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-28 / 2024-03-28

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ap-dos-h9TGGX6W
- https://bdu.fstec.ru/vul/2024-02369

10

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena Simulation

Идентификатор уязвимости: CVE-2024-21918

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Arena Simulation Software: 16.00

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/support/advisory.SD-1665.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03

11

Краткое описание: Отказ в обслуживании в Cisco IOS and IOS XE Software

Идентификатор уязвимости: CVE-2024-20308

Идентификатор программной ошибки: CWE-124 Запись данных в область перед началом буфера

Уязвимый продукт: Cisco IOS и Cisco IOS XE:
Cisco IOS: с версии 17.9.3 по 17.12.1
Cisco IOS XE: с версии 17.9.3 по 17.12.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-28 / 2024-03-28

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev1-NO2ccFWz

12

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena Simulation

Идентификатор уязвимости: CVE-2024-21913

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

Уязвимый продукт: Arena Simulation Software: 16.00

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/support/advisory.SD-1665.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03

13

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena Simulation

Идентификатор уязвимости: CVE-2024-21912

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Arena Simulation Software: 16.00

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://www.rockwellautomation.com/en-us/support/advisory.SD-1665.html
- http://www.cisa.gov/news-events/ics-advisories/icsa-24-086-03

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-2887

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 123.0.6312.59

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html
- http://crbug.com/330588502

15

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-2886

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 123.0.6312.59

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html
- http://crbug.com/330575496

16

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-2885

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по123.0.6312.59

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html
- http://crbug.com/328958020

17

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-2883

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 123.0.6312.59

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-27 / 2024-03-27

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/03/stable-channel-update-for-desktop_26.html
- http://crbug.com/327807820

18

Краткое описание: Выполнение произвольного кода в GNU Emacs

Идентификатор уязвимости: CVE-2024-30204

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Emacs: 29.0.90 - 29.2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-26 / 2024-03-26

Ссылки на источник:

- http://git.savannah.gnu.org/cgit/emacs.git/tree/etc/NEWS?h=emacs-29
- http://git.savannah.gnu.org/cgit/emacs.git/commit/?h=emacs-29&id=6f9ea396f49cbe38c2173e0a72ba6af3e03b271c

19

Краткое описание: Выполнение произвольного кода в GNU Emacs

Идентификатор уязвимости: CVE-2024-30203

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Emacs: 29.0.90 - 29.2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-26 / 2024-03-26

Ссылки на источник:

- http://git.savannah.gnu.org/cgit/emacs.git/tree/etc/NEWS?h=emacs-29
- http://git.savannah.gnu.org/cgit/emacs.git/commit/?h=emacs-29&id=937b9042ad7426acdcca33e3d931d8f495bdd804

20

Краткое описание: Выполнение произвольного кода в GNU Emacs

Идентификатор уязвимости: CVE-2024-30202

Идентификатор программной ошибки: CWE-676 Использование потенциально опасной функции

Уязвимый продукт: Emacs: 29.0.90 - 29.2

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-26 / 2024-03-26

Ссылки на источник:

- http://git.savannah.gnu.org/cgit/emacs.git/tree/etc/NEWS?h=emacs-29
- http://git.savannah.gnu.org/cgit/emacs/org-mode.git/commit/?id=003ddacf1c8d869b1858181c29ea21b731a8d8d9
- http://git.savannah.gnu.org/cgit/emacs.git/commit/?h=emacs-29&id=befa9fcaae29a6c9a283ba371c3c5234c7f644eb

21

Краткое описание: Получение конфиденциальной информации в GNU Emacs

Идентификатор уязвимости: CVE-2024-30205

Идентификатор программной ошибки: CWE-345 Некорректная проверка достоверности данных

Уязвимый продукт: Emacs: 29.0.90 - 29.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-26 / 2024-03-26

Ссылки на источник:

- http://git.savannah.gnu.org/cgit/emacs.git/tree/etc/NEWS?h=emacs-29
- http://git.savannah.gnu.org/cgit/emacs/org-mode.git/commit/?id=4255d5dcc0657915f90e4fba7e0a5514cced514d
- http://git.savannah.gnu.org/cgit/emacs.git/commit/?h=emacs-29&id=2bc865ace050ff118db43f01457f95f95112b877

Краткое описание: Повышение привилегий в Podman

Идентификатор уязвимости: CVE-2024-1753

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Podman: 4.9.0 - 4.9.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-26 / 2024-03-26

Ссылки на источник:

- http://github.com/containers/libpod/releases/tag/v4.9.4
- https://bdu.fstec.ru/vul/2024-02163

Краткое описание: Выполнение произвольного кода в macOS Sonoma, macOS Ventura и Apple Safari

Идентификатор уязвимости: CVE-2024-1580

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

Уязвимый продукт: macOS Sonoma: 14.0 23A344 - 14.4 23E214
macOS Ventura: 13.0 22A380 - 13.6.5 22G621
Apple Safari: 15.0 - 17.4

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-03-26 / 2024-03-26

Ссылки на источник:

- http://support.apple.com/en-us/HT214096
- http://support.apple.com/en-us/HT214095
- http://support.apple.com/en-us/HT214094