НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-06-05.1 | 5 июня 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-4577	PHP	Сетевой	ACE	2024-06-05	✓
2	Высокая	CVE-2024-5585	PHP	Сетевой	ACE	2024-06-05	✓
3	Высокая	CVE-2024-28996	SolarWinds Orion Platform	Смежная сеть	ACE	2024-06-04	✓
4	Критическая	CVE-2024-34852	F-logic DataCube3	Сетевой	ACE	2024-06-04	✗
5	Высокая	CVE-2024-34854	F-logic DataCube3	Сетевой	WLF	2024-06-04	✗
6	Критическая	CVE-2024-36843	libmodbus	Сетевой	ACE	2024-06-04	✓
7	Высокая	CVE-2024-5274	Google ChromeOS	Сетевой	ACE	2024-06-04	✓
8	Высокая	CVE-2024-5158	Google ChromeOS	Сетевой	ACE	2024-06-04	✓
9	Высокая	CVE-2024-5499	Google Chrome	Сетевой	ACE	2024-06-04	✓
10	Высокая	CVE-2024-5498	Google Chrome	Сетевой	ACE	2024-06-04	✓
11	Высокая	CVE-2024-5497	Google Chrome	Сетевой	ACE	2024-06-04	✓
12	Высокая	CVE-2024-5496	Google Chrome	Сетевой	ACE	2024-06-04	✓
13	Высокая	CVE-2024-5495	Google Chrome	Сетевой	ACE	2024-06-04	✓

14	Высокая	CVE-2024-5494	Google Chrome	Сетевой	ACE	2024-06-04	✓
15	Высокая	CVE-2024-5493	Google Chrome	Сетевой	ACE	2024-06-04	✓
16	Критическая	CVE-2024-5154	CRI-O	Сетевой	PE	2024-06-04	✓
17	Критическая	CVE-2024-25180	pdfmake	Сетевой	ACE	2024-06-03	✓
18	Критическая	None	libvpx	Сетевой	ACE	2024-05-31	✓
19	Критическая	CVE-2024-5197	libvpx	Сетевой	ACE	2024-05-31	✓
20	Критическая	None	libvpx	Сетевой	DoS	2024-05-31	✓
21	Высокая	CVE-2024-4990	Yii	Сетевой	ACE	2024-05-31	✓
22	Критическая	CVE-2024-36246	Unifier and Unifier Cast	Сетевой	OAF	2024-05-28	✓
23	Высокая	CVE-2024-23847	Unifier and Unifier Cast	Локальный	ACE	2024-05-28	✓
24	Критическая	CVE-2024-5035	TP-Link Archer C5400X	Сетевой	ACE	2024-05-28	✓
25	Высокая	CVE-2024-24919	Check Point Quantum Gateway, Check Point Spark и CloudGuard Network	Сетевой	OSI	2024-05-29	✓

1

Краткое описание: Выполнение произвольного кода в PHP

Идентификатор уязвимости: CVE-2024-4577

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

Уязвимый продукт: PHP: 5 - 8.3.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.1 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://github.com/php/php-src/security/advisories/GHSA-3qgc-jrrr-25jv

2

Краткое описание: Выполнение произвольного кода в PHP

Идентификатор уязвимости: CVE-2024-5585

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

Уязвимый продукт: PHP: 8.2.0 - 8.3.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-06-05 / 2024-06-05

Ссылки на источник:

- http://github.com/php/php-src/security/advisories/GHSA-9fcc-425m-g385

3

Краткое описание: Выполнение произвольного кода в SolarWinds Orion Platform

Идентификатор уязвимости: CVE-2024-28996

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

Уязвимый продукт: Orion Platform: 2016.1 - 2024.1.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://www.solarwinds.com/trust-center/security-advisories/cve-2024-28996

4

Краткое описание: Выполнение произвольного кода в F-logic DataCube3

Идентификатор уязвимости: CVE-2024-34852

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

Уязвимый продукт: DataCube3: 1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://github.com/Yang-Nankai/Vulnerabilities/blob/main/DataCube3%20Shell%20Code%20Injection.md

Краткое описание: Запись локальных файлов в F-logic DataCube3

Идентификатор уязвимости: CVE-2024-34854

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

Уязвимый продукт: DataCube3: 1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

5

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://github.com/Yang-Nankai/Vulnerabilities/blob/main/DataCube3%20Shell%20Code%20Injection.md

6

Краткое описание: Выполнение произвольного кода в libmodbus

Идентификатор уязвимости: CVE-2024-36843

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

Уязвимый продукт: libmodbus: 3.1.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://github.com/stephane/libmodbus/issues/748

7

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-5274

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

Уязвимый продукт: Chrome OS: до 120.0.6099.313

Категория уязвимого продукта: Unix-подобные операционные системы 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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/long-term-support-channel-update-for.html

8

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2024-5158

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

Уязвимый продукт: Chrome OS: до 120.0.6099.313

Категория уязвимого продукта: Unix-подобные операционные системы 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/long-term-support-channel-update-for.html

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5499

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/339877167

10

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5498

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/339588211

11

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5497

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/339061099

12

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5496

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/338929744

13

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5495

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/338103465

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5494

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/338071106

15

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-5493

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 125.0.6422.114

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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
- http://crbug.com/339877165

Краткое описание: Повышение привилегий в CRI-O

Идентификатор уязвимости: CVE-2024-5154

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: CRI-O: 1.28.6 - 1.30.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

16 **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: 2024-06-04 / 2024-06-04

Ссылки на источник:

- http://github.com/cri-o/cri-o/security/advisories/GHSA-j9hf-98c3-wrm8

17

Краткое описание: Выполнение произвольного кода в pdfmake

Идентификатор уязвимости: CVE-2024-25180

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

Уязвимый продукт: pdfmake: 0.2.9

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://github.com/joaoviictorti/My-CVES/blob/main/CVE-2024-25180/README.md
- http://www.youtube.com/watch?v=QcOlrWUGo6o
- http://security.snyk.io/vuln/SNYK-JS-PDFMAKE-6347243
- http://github.com/bpampuch/pdfmake/issues/2702

Краткое описание: Выполнение произвольного кода в libvpx

Идентификатор уязвимости: None

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

Уязвимый продукт: libvpx: 1.14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-05-31 / 2024-05-31

Ссылки на источник:

- http://github.com/webmproject/libvpx/releases/tag/v1.14.1

Краткое описание: Выполнение произвольного кода в libvpx

Идентификатор уязвимости: CVE-2024-5197

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

Уязвимый продукт: libvpx: 1.14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-05-31 / 2024-05-31

Ссылки на источник:

- http://github.com/webmproject/libvpx/releases/tag/v1.14.1

Краткое описание: Отказ в обслуживании в libvpx

Идентификатор уязвимости: None

Идентификатор программной ошибки: CWE-369 Деление на ноль

Уязвимый продукт: libvpx: 1.14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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: 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: 2024-05-31 / 2024-05-31

Ссылки на источник:

- http://github.com/webmproject/libvpx/releases/tag/v1.14.1

Краткое описание: Выполнение произвольного кода в Yii

Идентификатор уязвимости: CVE-2024-4990

Идентификатор программной ошибки: CWE-470 Использование внешних входных данных для выбора класса или кода ("небезопасное отражение")

Уязвимый продукт: Yii: 2.0.0 - 2.0.49

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-05-31 / 2024-05-31

Ссылки на источник:

- http://github.com/yiisoft/yii2/security/advisories/GHSA-cjcc-p67m-7qxm

Краткое описание: Перезапись произвольных файлов в Unifier and Unifier Cast

Идентификатор уязвимости: CVE-2024-36246

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Unifier: до 6 patch 20240527
Unifier Cast: до 6 patch 20240527

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Выполнение специально созданного вредоносного файла

Последствия эксплуатации: Перезапись произвольных 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: 2024-05-28 / 2024-05-28

Ссылки на источник:

- http://jvn.jp/en/jp/JVN17680667/index.html
- http://www.yrl.com/fwp_support/info/khvu7f00000000q7.html

Краткое описание: Выполнение произвольного кода в Unifier and Unifier Cast

Идентификатор уязвимости: CVE-2024-23847

Идентификатор программной ошибки: CWE-276 Некорректные разрешения, назначаемые по умолчанию

Уязвимый продукт: Unifier: до 6 patch 20240527
Unifier Cast: до 6 patch 20240527

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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: 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: 2024-05-28 / 2024-05-28

Ссылки на источник:

- http://jvn.jp/en/jp/JVN17680667/index.html
- http://www.yrl.com/fwp_support/info/khvu7f00000000q7.html

Краткое описание: Выполнение произвольного кода в TP-Link Archer C5400X

Идентификатор уязвимости: CVE-2024-5035

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

Уязвимый продукт: Archer C4500X: 1_1.1.4 - 1_1.1.6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-28 / 2024-05-28

Ссылки на источник:

- http://onekey.com/blog/security-advisory-remote-command-execution-on-tp-link-archer-c5400x/
- http://www.tp-link.com/en/support/download/archer-c5400x/#Firmware

Краткое описание: Получение конфиденциальной информации в Check Point Quantum Gateway, Check Point Spark и CloudGuard Network

Идентификатор уязвимости: CVE-2024-24919

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

Уязвимый продукт: Check Point Quantum Gateway, Check Point Spark и CloudGuard Network:
Check Point Quantum Gateway: R81.20
Check Point Quantum Gateway: R81.10
Check Point Quantum Gateway: R81
Check Point Quantum Gateway: R80.40
CloudGuard Network: R81.20
CloudGuard Network: R81.10
CloudGuard Network: R81
CloudGuard Network: R80.40
Check Point Spark: R81.10
Check Point Spark: R80.20

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-29 / 2024-05-29

Ссылки на источник:

- https://bdu.fstec.ru/vul/2024-04175
- http://support.checkpoint.com/results/sk/sk182336
- http://blog.checkpoint.com/security/enhance-your-vpn-security-posture