НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-06-26.1 | 26 июня 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Не определено	CVE-2023-32435	Apple iOS, iPadOS	Не определено	ACE	2023-06-21	✓
2	Высокая	CVE-2023-3256	Advantech R-SeeNet	Сетевой	RLF	2023-06-23	✓
3	Критическая	CVE-2023-2611	Advantech R-SeeNet	Сетевой	SB	2023-06-23	✓
4	Высокая	CVE-2023-20895	vCenter Server	Сетевой	OSI	2023-06-22	✓
5	Высокая	CVE-2023-20894	VMWare vCenter Server	Сетевой	ACE	2023-06-22	✓
6	Высокая	CVE-2023-20893	VMWare vCenter Server	Сетевой	ACE	2023-06-22	✓
7	Высокая	CVE-2023-20892	VMWare vCenter Server	Сетевой	ACE	2023-06-22	✓
8	Критическая	CVE-2023-3128	Grafana	Сетевой	SB	2023-06-22	✓
9	Высокая	CVE-2023-32233	Chrome OS	Локальный	ACE	2023-06-21	✓
10	Высокая	CVE-2023-2935	Chrome OS	Сетевой	ACE	2023-06-21	✓
11	Высокая	CVE-2023-3079	Chrome OS	Сетевой	ACE	2023-06-21	✓
12	Не определено	CVE-2023-32439	Apple Safari, macOS Ventura, Apple iOS, iPadOS	Не определено	ACE	2023-06-21	✓
13	Не определено	CVE-2023-32434	Apple iOS, iPadOS, MacOS	Не определено	ACE	2023-06-21	✓

Краткое описание: Выполнение произвольного кода в Apple iOS, iPadOS

Идентификатор уязвимости: CVE-2023-32435

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

Уязвимый продукт: Apple iOS, iPadOS:
Apple iOS 15.0 19A346 - 15.7.6 19H349
iPadOS 15.0 19A346 - 15.7.6 19H349

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

1 **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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://support.apple.com/en-us/HT213811

2

Краткое описание: Чтение локальных файлов в Advantech R-SeeNet

Идентификатор уязвимости: CVE-2023-3256

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: Advantech R-SeeNet: 2.4.22 - 2.4.22

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-23 / 2023-06-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-173-02

3

Краткое описание: Обход безопасности в Advantech R-SeeNet

Идентификатор уязвимости: CVE-2023-2611

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Advantech R-SeeNet: 2.4.22 - 2.4.22

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-23 / 2023-06-23

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-173-02

Краткое описание: Получение конфиденциальной информации в vCenter Server

Идентификатор уязвимости: CVE-2023-20895

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: vCenter Server: 7.0 - 8.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

4 **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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-22

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0014.html

5

Краткое описание: Выполнение произвольного кода в VMWare vCenter Server

Идентификатор уязвимости: CVE-2023-20894

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMWare vCenter Server: 7.0 - 8.0c

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-22

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0014.html

6

Краткое описание: Выполнение произвольного кода в VMWare vCenter Server

Идентификатор уязвимости: CVE-2023-20893

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: VMWare vCenter Server: 7.0 - 8.0c

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-22

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0014.html

7

Краткое описание: Выполнение произвольного кода в VMWare vCenter Server

Идентификатор уязвимости: CVE-2023-20892

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

Уязвимый продукт: VMWare vCenter Server: 7.0 - 8.0c

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: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-22

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0014.html

Краткое описание: Обход безопасности в Grafana

Идентификатор уязвимости: CVE-2023-3128

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Grafana: 9.2.0 - 9.3.15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

8

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-22

Ссылки на источник:

- http://github.com/grafana/grafana/releases/tag/v9.3.16
- http://github.com/grafana/grafana/releases/tag/v9.2.20
- http://grafana.com/security/security-advisories/cve-2023-3128/

9

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-32233

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 108.0.5359.235

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

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/06/long-term-support-channel-update-for_21.html
- https://bdu.fstec.ru/vul/2023-02625

10

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-2935

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

Уязвимый продукт: Chrome OS: до 108.0.5359.235

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/06/long-term-support-channel-update-for_21.html

11

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-3079

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

Уязвимый продукт: Chrome OS: до 108.0.5359.235

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

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/06/long-term-support-channel-update-for_21.html
- https://bdu.fstec.ru/vul/2023-03080

Краткое описание: Выполнение произвольного кода в Apple Safari, macOS Ventura, Apple iOS, iPadOS

Идентификатор уязвимости: CVE-2023-32439

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

Уязвимый продукт: Apple Safari, macOS Ventura, Apple iOS, iPadOS:
macOS Ventura 13.0 22A380 - 13.4 22F66
Apple Safari 16.0 - 16.5
Apple iOS 15.0 19A346 - 15.7.6 19H349
iPadOS 15.0 19A346 - 15.7.6 19H349

Категория уязвимого продукта: Операционные системы Apple 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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://support.apple.com/en-us/HT213813
- http://support.apple.com/en-us/HT213816
- http://support.apple.com/en-us/HT213811
- https://bdu.fstec.ru/vul/2023-03342

Краткое описание: Выполнение произвольного кода в Apple iOS, iPadOS, MacOS

Идентификатор уязвимости: CVE-2023-32434

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

Уязвимый продукт: Apple iOS, iPadOS, MacOS:
Apple iOS 15.0 19A346 - 15.7.6 19H349
iPadOS 15.0 19A346 - 15.7.6 19H349
macOS Ventura 13.0 22A380 - 13.4 22F66
macOS Monterey 12.0 21A344 - 12.6.6
macOS Big Sur 11.0 20A2411 - 11.7.7

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-21 / 2023-06-21

Ссылки на источник:

- http://support.apple.com/en-us/HT213813
- http://support.apple.com/en-us/HT213811
- http://support.apple.com/en-us/HT213810
- http://support.apple.com/en-us/HT213809
- https://bdu.fstec.ru/vul/2023-03341