НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-22.1 | 22 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2023-2071	Rockwell Automation FactoryTalk View Machine Edition	Сетевой	ACE	2023-09-22	✓
2	Критическая	CVE-2023-41991	macOS Ventura	Сетевой	SB	2023-09-21	✓
3	Критическая	CVE-2023-41992	macOS Monterey и Ventura	Сетевой	PE, ACE	2023-09-21	✓
4	Критическая	CVE-2023-41993	WebKitGTK+ и WPE WebKit, Apple Safari, macOS Ventura	Сетевой	ACE	2023-09-21	✗

1

Краткое описание: Выполнение произвольного кода в Rockwell Automation FactoryTalk View Machine Edition

Идентификатор уязвимости: CVE-2023-2071

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Rockwell Automation FactoryTalk View Machine Edition: 12.0 - 13.0

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: 2023-09-22 / 2023-09-22

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140724
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-264-06
- https://bdu.fstec.ru/vul/2023-05917

2

Краткое описание: Обход безопасности в macOS Ventura

Идентификатор уязвимости: CVE-2023-41991

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: macOS Ventura: 13.0 22A380 - 13.5.2 22G91

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-09-21 / 2023-09-21

Ссылки на источник:

- http://support.apple.com/en-us/HT213931

3

Краткое описание: Повышение привилегий в macOS Monterey и Ventura

Идентификатор уязвимости: CVE-2023-41992

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS Monterey и Ventura:
macOS Monterey: 12.0 21A344 - 12.6.9 21G726
macOS Ventura: 13.0 22A380 - 13.5.2 22G91

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: повышение привилегий, 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: 9.1 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: 2023-09-21 / 2023-09-21

Ссылки на источник:

- http://support.apple.com/en-us/HT213932
- http://support.apple.com/en-us/HT213931

4

Краткое описание: Выполнение произвольного кода в WebKitGTK+ и WPE WebKit, Apple Safari, macOS Ventura

Идентификатор уязвимости: CVE-2023-41993

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

Уязвимый продукт: WebKitGTK+ и WPE WebKit, Apple Safari, macOS Ventura:
WebKitGTK+ и WPE WebKit: Все версии
Apple Safari: 16.0 - 16.6
macOS Ventura: 13.0 22A380 - 13.5.2 22G91

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

Последствия эксплуатации: выполнение произвольного кода

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

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: 2023-09-21 / 2023-09-21

Ссылки на источник:

- http://support.apple.com/en-us/HT213927
- http://support.apple.com/en-us/HT213930
- http://support.apple.com/en-us/HT213931