НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-10-27.1 | 27 октября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-46290	Rockwell Automation FactoryTalk Services Platform	Сетевой	SB	2023-10-27	✓
2	Высокая	CVE-2023-34058	VMware Tools	Смежная сеть	OSI	2023-10-27	✓
3	Высокая	CVE-2023-27858	Rockwell Automation Arena	Локальный	ACE	2023-10-27	✓
4	Высокая	CVE-2023-27854	Rockwell Automation Arena	Локальный	OSI	2023-10-27	✓
5	Критическая	CVE-2023-42854	macOS Monterey	Сетевой	DoS	2023-10-25	✓
6	Высокая	CVE-2023-42852	Apple Safari	Сетевой	ACE	2023-10-25	✓
7	Высокая	CVE-2023-41976	Apple Safari	Сетевой	ACE	2023-10-25	✓
8	Высокая	CVE-2023-40447	Apple Safari	Сетевой	ACE	2023-10-25	✓
9	Высокая	CVE-2023-40447	WebKitGTK+	Сетевой	ACE	2023-10-25	✗
10	Высокая	CVE-2023-41976	WebKitGTK+	Сетевой	ACE	2023-10-25	✗
11	Высокая	CVE-2023-42852	WebKitGTK+	Сетевой	ACE	2023-10-25	✗
12	Высокая	CVE-2023-5246	Bosch Rexroth SLC-0-GPNT00300	Сетевой	SB	2023-10-25	✗
13	Высокая	CVE-2023-5246	SICK Flexi Soft Gateways	Сетевой	SB	2023-10-25	✓

14	Критическая	CVE-2023-34048	VMware vCenter Server	Сетевой	ACE	2023-10-25	✓
15	Высокая	CVE-2023-5535	Vim	Локальный	ACE	2023-10-24	✓
16	Высокая	CVE-2023-20273	Cisco IOS XE	Сетевой	PE	2023-10-17	✓
17	Критическая	CVE-2023-20198	Cisco IOS XE и Rockwell Automation Stratix 5800, Stratix 5200 под управлением Cisco IOS XE	Сетевой	PE	2023-10-17	✓

1

Краткое описание: Обход безопасности в Rockwell Automation FactoryTalk Services Platform

Идентификатор уязвимости: CVE-2023-46290

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Rockwell Automation FactoryTalk Services Platform: 2.74

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.

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: 2023-10-27 / 2023-10-27

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-299-06

2

Краткое описание: Получение конфиденциальной информации в VMware Tools

Идентификатор уязвимости: CVE-2023-34058

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: VMware Tools: 10.3.0 - 12.3.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2023-10-27 / 2023-10-27

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0024.html

3

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena

Идентификатор уязвимости: CVE-2023-27858

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Rockwell Automation Arena: 16.20.00001

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка 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: 2023-10-27 / 2023-10-27

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-299-04

4

Краткое описание: Получение конфиденциальной информации в Rockwell Automation Arena

Идентификатор уязвимости: CVE-2023-27854

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Rockwell Automation Arena: 16.20.00001

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 2023-10-27 / 2023-10-27

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-23-299-04

Краткое описание: Отказ в обслуживании в macOS Monterey

Идентификатор уязвимости: CVE-2023-42854

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: macOS Monterey: 12.0 21A344 - 12.7 21G816
macOS Sonoma: 14.0 23A344

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: отказ в обслуживании

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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213983
- http://support.apple.com/en-us/HT213984

6

Краткое описание: Выполнение произвольного кода в Apple Safari

Идентификатор уязвимости: CVE-2023-42852

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apple Safari: 17.0

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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213986

Краткое описание: Выполнение произвольного кода в Apple Safari

Идентификатор уязвимости: CVE-2023-41976

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Apple Safari: 17.0

Категория уязвимого продукта: Операционные системы Apple и их компоненты

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

Последствия эксплуатации: выполнение произвольного кода

7 **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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213986

8

Краткое описание: Выполнение произвольного кода в Apple Safari

Идентификатор уязвимости: CVE-2023-40447

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

Уязвимый продукт: Apple Safari: 17.0

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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213986

9

Краткое описание: Выполнение произвольного кода в WebKitGTK+

Идентификатор уязвимости: CVE-2023-40447

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

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213986

10

Краткое описание: Выполнение произвольного кода в WebKitGTK+

Идентификатор уязвимости: CVE-2023-41976

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213986

11

Краткое описание: Выполнение произвольного кода в WebKitGTK+

Идентификатор уязвимости: CVE-2023-42852

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://support.apple.com/en-us/HT213986

Краткое описание: Обход безопасности в Bosch Rexroth SLC-0-GPNT00300

Идентификатор уязвимости: CVE-2023-5246

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: Bosch Rexroth SLC-0-GPNT00300: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: обход безопасности

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

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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://psirt.bosch.com/security-advisories/bosch-sa-164691.html

13

Краткое описание: Обход безопасности в SICK Flexi Soft Gateways

Идентификатор уязвимости: CVE-2023-5246

Идентификатор программной ошибки: CWE-294 Обход аутентификации при помощи перехвата и воспроизведения

Уязвимый продукт: SICK Flexi Soft Gateways:
SICK FX0-GENT00000: все версии
SICK FX0-GENT00010: все версии
SICK FX0-GENT00030: все версии
SICK FX0-GETC00000: все версии
SICK FX0-GETC00010: все версии
SICK FX0-GMOD00000: все версии
SICK FX0-GMOD00010: все версии
SICK FX0-GMOD00030: все версии
SICK FX0-GPNT00000: все версии
SICK FX0-GPNT00010: все версии
SICK FX0-GPNT00030: все версии
SICK FX3-GEPR00000: все версии
SICK FX3-GEPR00010: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://sick.com/.well-known/csaf/white/2023/sca-2023-0011.pdf

- http://sick.com/psirt
- http://sick.com/.well-known/csaf/white/2023/sca-2023-0011.json

Краткое описание: Выполнение произвольного кода в VMware vCenter Server

Идентификатор уязвимости: CVE-2023-34048

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMware vCenter Server: 7.0 U1 - 8.0.0c

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: выполнение произвольного кода

14 **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: 2023-10-25 / 2023-10-25

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0023.html

Краткое описание: Выполнение произвольного кода в Vim

Идентификатор уязвимости: CVE-2023-5535

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Vim: до 9.0.2010

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.

15

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: 2023-10-24 / 2023-10-24

Ссылки на источник:

- http://github.com/vim/vim/commit/41e6f7d6ba67b61d911f9b1d76325cd79224753d
- http://huntr.dev/bounties/2c2d85a7-1171-4014-bf7f-a2451745861f
- http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VDDWD25AZIHBAA44HQT75OWLQ5UMDKU3/
- http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VGTVLUV7UCXXCZAIQIUCLG6JXAVYT3HE/

Краткое описание: Повышение привилегий в Cisco IOS XE

Идентификатор уязвимости: CVE-2023-20273

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Cisco IOS XE: до 17.9.4a

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-17 / 2023-10-17

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j...

Краткое описание: Повышение привилегий в Cisco IOS XE и Rockwell Automation Stratix 5800, Stratix 5200 под управлением Cisco IOS XE

Идентификатор уязвимости: CVE-2023-20198

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Cisco IOS XE и Rockwell Automation Stratix 5800, Stratix 5200 под управлением Cisco IOS XE:
Cisco IOS XE: до 17.9.4a
Stratix 5200: Все версии
Stratix 5800: Все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: повышение привилегий

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-10-17 / 2023-10-17

Ссылки на источник:

- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh87343
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-297-01
- http://www.rockwellautomation.com/en-in/support/advisory.PN1653.html
- https://bdu.fstec.ru/vul/2023-06875