НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-08-30.1 | 30 августа 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-40031	Notepad++	Локальный	ACE	2023-08-25	✗
2	Высокая	CVE-2023-20890	VMware Aria Operations for Networks (formerly vRealize Network Insight)	Сетевой	WLF	2023-08-29	✓
3	Критическая	CVE-2023-34039	VMware Aria Operations for Networks (formerly vRealize Network Insight)	Сетевой	SB	2023-08-29	✓
4	Критическая	CVE-2023-2917	Rockwell Automation ThinManager and ThinServer	Сетевой	WLF	2023-08-28	✓
5	Высокая	CVE-2023-2915	Rockwell Automation ThinManager and ThinServer	Сетевой	OSI	2023-08-28	✓
6	Высокая	CVE-2023-2914	Rockwell Automation ThinManager and ThinServer	Сетевой	DoS	2023-08-28	✓
7	Высокая	CVE-2023-38831	WinRAR	Локальный	ACE	2023-08-23	✓

1

Краткое описание: Выполнение произвольного кода в Notepad++

Идентификатор уязвимости: CVE-2023-40031

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Notepad++: до 8.5.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2023-08-25 / 2023-08-26

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-40031

2

Краткое описание: Запись локальных файлов в VMware Aria Operations for Networks (formerly vRealize Network Insight)

Идентификатор уязвимости: CVE-2023-20890

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

Уязвимый продукт: VMware Aria Operations for Networks (formerly vRealize Network Insight): до 6.11

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Запись 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: 7.2 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: 2023-08-29 / 2023-08-29

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0018.html
- http://kb.vmware.com/s/article/94152

3

Краткое описание: Обход безопасности в VMware Aria Operations for Networks (formerly vRealize Network Insight)

Идентификатор уязвимости: CVE-2023-34039

Идентификатор программной ошибки: CWE-338 Использование ненадежного ГПСЧ

Уязвимый продукт: VMware Aria Operations for Networks (formerly vRealize Network Insight): до 6.11

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

Дата выявления / Дата обновления: 2023-08-29 / 2023-08-29

Ссылки на источник:

- http://www.vmware.com/security/advisories/VMSA-2023-0018.html
- http://kb.vmware.com/s/article/94152

Краткое описание: Запись локальных файлов в Rockwell Automation ThinManager and ThinServer

Идентификатор уязвимости: CVE-2023-2917

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

Уязвимый продукт: Rockwell Automation ThinManager and ThinServer:
ThinManager: 11.0.0 - 13.1.0
ThinServer: 11.0.0 - 13.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Запись локальных файлов

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: 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: 2023-08-28 / 2023-08-28

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140471
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-234-03
- https://bdu.fstec.ru/vul/2023-04836

Краткое описание: Получение конфиденциальной информации в Rockwell Automation ThinManager and ThinServer

Идентификатор уязвимости: CVE-2023-2915

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

Уязвимый продукт: Rockwell Automation ThinManager and ThinServer:
ThinManager: 11.0.0 - 13.1.0
ThinServer: 11.0.0 - 13.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-28 / 2023-08-28

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140471
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-234-03
- https://bdu.fstec.ru/vul/2023-04844

Краткое описание: Отказ в обслуживании в Rockwell Automation ThinManager and ThinServer

Идентификатор уязвимости: CVE-2023-2914

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Rockwell Automation ThinManager and ThinServer:
ThinManager: 11.0.0 - 13.1.0
ThinServer: 11.0.0 - 13.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

6 **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:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2023-08-28 / 2023-08-28

Ссылки на источник:

- http://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140471
- http://www.cisa.gov/news-events/ics-advisories/icsa-23-234-03
- https://bdu.fstec.ru/vul/2023-04775

Краткое описание: Выполнение произвольного кода в WinRAR

Идентификатор уязвимости: CVE-2023-38831

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: WinRAR: 3.20 - 6.23 beta 1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2023-08-23 / 2023-08-29

Ссылки на источник:

- http://www.group-ib.com/blog/cve-2023-38831-winrar-zero-day/