НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220901.4 | 1 сентября 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в IBM Spectrum Discover

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Spectrum Discover: 2.0.4 - 2.0.4.4
Дата выявления	22 августа 2022 г.
Дата обновления	22 августа 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-41092	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД в целевой системе. Уязвимость обусловлена некорректным выводом данных приложением. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-200: Разглашение важной информации лицам без соответствующих прав 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.	7.5

MITRE: CVE-2021-4104	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных 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.	8.1
MITRE: CVE-2022-23302	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных 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.	9.8
MITRE: CVE-2022-23307 CVE-2020-9493	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных 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.	9.8

Ссылки на источники	http://www.ibm.com/blogs/psirt/security-bulletin-ibm-spectrum-discover-is-vulnerable-to-docker-cli-cve-2021-41092-and-apache-log4j-cve-2021-4104-cve-2022-23302-cve-2022-23305-cve-2022-23307-weaknesses-2/ http://www.ibm.com/support/pages/node/6568675