НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220713.2 | 13 июля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегии в IBM App Connect Enterprise и IBM Integration Bus

Идентификатор уязвимости	MITRE: CVE-2021-44906
Идентификатор программной ошибки	CWE-400: Неконтролируемое использование ресурсов (исчерпание ресурсов)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить привилегии в целевой системе. Уязвимость обусловлена некорректным использованием внутренних ресурсов.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IBM Integration Bus: 10.0.0.0 - 10.0.0.26 IBM App Connect Enterprise: 11.0.0.0 - 12.0.3.0
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.
Дата выявления	05 июля 2022 г.
Дата обновления	05 июля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)

Масштаб последствий эксплуатации уязвимости (S)	Не изменяется (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	http://www.ibm.com/support/pages/node/6601101