НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20221005.3 | 5 октября 2022 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в IBM Cloud Pak for Business Automation

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IBM Cloud Pak for Business Automation: до 22.0.1-IF001
Дата выявления	22 сентября 2022 г.
Дата обновления	22 сентября 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-23017	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой в функции обработки ответов DNS. CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L CWE-193: Ошибка смещения на единицу 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.	7.7

MITRE: CVE-2021-23019	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена хранением важных данных в незашифрованном виде. CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CWE-312: Хранение важных данных в незашифрованном виде 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.	7.8

Ссылки на источники	http://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-f5-nginx-controller-affect-ibm-cloud-pak-for-automation/ http://www.ibm.com/support/pages/node/6473495