НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230210.2 | 10 февраля 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Обход безопасности в IBM Watson Discovery for IBM Cloud Pak for Data

Идентификатор уязвимости	MITRE: CVE-2022-23491
Идентификатор программной ошибки	CWE-345: Некорректная проверка достоверности данных
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику обойти проверку сертификата посредством отправки специально созданного запроса. Уязвимость обусловлена некорректной проверкой данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IBM Watson Discovery for IBM Cloud Pak for Data: до 4.6.2
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	9 февраля 2023 г.
Дата обновления	9 февраля 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	6.8 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)

Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Отсутствует (N)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Отсутствует (N)
Степень зрелости доступных средств эксплуатации	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	http://www.ibm.com/support/pages/node/6855127