

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)  
E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220713.12 | 13 июля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в IBM Tivoli Netcool Impact

Идентификатор уязвимости	MITRE: CVE-2022-22965
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	IBM Tivoli Netcool Impact: 7.1.0 - 7.1.0.25
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	06 июля 2022 г.
Дата обновления	06 июля 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Отсутствует (N)
Необходимость взаимодействия с	Отсутствует (N)

пользователем (UI)

Масштаб последствий эксплуатации уязвимости (S)

Изменяется (C)

Влияние на конфиденциальность (C)

Высокое (H)

Влияние на целостность (I)

Высокое (H)

Влияние на доступность (A)

Высокое (H)

Степень зрелости доступных средств эксплуатации

Высокая

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

---

Ссылки на источники

<http://www.ibm.com/blogs/psirt/security-bulletin-ibm-tivoli-netcool-impact-is-affected-but-not-classified-as-vulnerable-by-a-remote-code-execution-in-spring-framework-cve-2022-22965/>  
<http://www.ibm.com/support/pages/node/6601301>