

# 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-20220222.10 | 22 февраля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в IBM WebSphere Application Server

Идентификатор уязвимости	MITRE: CVE-2022-23302 CVE-2022-23307 CVE-2020-9493
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных
Описание уязвимости	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.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	IBM WebSphere Application Server Liberty: 21.0.0.1 - 21.0.0.12 Сервер приложений IBM WebSphere: 7.0.0.0–9.0.5.10
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	18 января 2022 г.
Дата обновления	18 января 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
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	Не изменяется (U)

уязвимости (S)

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

<https://www.cybersecurity-help.cz/vdb/SB2022022130>  
<http://www.ibm.com/blogs/psirt/security-bulletin-ibm-websphere-application-server-and-ibm-websphere-application-server-liberty-are-vulnerable-to-arbitrary-code-execution-and-sql-injection-due-to-apache-log4j-cve-2022-23302-cve/>  
<http://www.ibm.com/support/pages/node/6557248>

Ссылки на источники