

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](http://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200623.2 | 23 июня 2020 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Подделка запросов в ПО IBM Maximo Asset Management

Идентификатор уязвимости	MITRE: CVE-2020-4529
Идентификатор программной ошибки	CWE-918: Подделка запроса со стороны сервера
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить подделку запросов на стороне сервера (SSRF-атака).
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимое ПО	IBM Maximo Asset Management до v7.6.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	5 июня 2020 г.
Дата обновления	5 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	7.4 AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Низкий (L)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации уязвимости (S)	Изменяется (C)
Влияние на конфиденциальность (C)	Низкое (L)
Влияние на целостность (I)	Низкое (L)
Влияние на доступность (A)	Низкое (L)

Степень зрелости доступных средств эксплуатации

Наличие не подтверждено

Наличие средств устранения уязвимости

Официальное решение

Достоверность сведений об уязвимости

Сведения подтверждены

<https://www.ibm.com/support/pages/node/6220528>

Ссылки на источники