

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200623.7 | 23 июня 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **НЕТ**

Выполнение произвольного кода в FasterXML

Идентификатор уязвимости	MITRE: CVE-2020-14060 CVE-2020-14061 CVE-2020-14062 CVE-2020-14195
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 вредоносных данных в уязвимое приложение. Уязвимость обусловлена некорректной проверкой при обработке сериализованных данных.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимое ПО	jackson-databind до v2.9.10.4
Рекомендации по устранению	На данный момент отсутствуют
Дата выявления	18 июня 2020 г.
Дата обновления	18 июня 2020 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C
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 уязвимости (S)	Не изменяется (U)
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	Недоступно
Достоверность сведений об уязвимости	Сведения подтверждены

Ссылки на источники

<https://www.cybersecurity-help.cz/vdb/SB2020061806>
<https://medium.com/@cowtowncoder/on-jackson-cves-dont-panic-here-is-what-you-need-to-know-54cd0d6e8062>