НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200319.5| 19 марта 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Red Hat Process Automation Manager

Идентификатор уязвимости	MITRE: CVE-2019-14892 CVE-2019-14893 CVE-2019-16942 CVE-2019-16943
Идентификатор программной ошибки	CWE-502: Десериализация недоверенных данных CWE-20: Некорректная проверка входных данных
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной работой элемента jackson-databind.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимое ПО	Red Hat Process Automation Manager (ранее JBoss BPM Suite): 7.0.0, 7.1.0, 7.2.0, 7.3.0, 7.4.0, 7.5.0, 7.6.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	2 марта 2020 г.
Дата обновления	19 марта 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
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	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2020031901 https://access.redhat.com/security/cve/CVE-2019-14892 https://access.redhat.com/security/cve/CVE-2019-14893 https://access.redhat.com/security/cve/CVE-2019-16942 https://access.redhat.com/security/cve/CVE-2019-16943