НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220217.2 | 17 февраля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Множественные уязвимости в Red Hat JBoss Web Server 3.1

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	JBoss Web Server: до 3.1.13 tomcat8 (Red Hat package): до 8.0.36-45.ep7.el7 tomcat7 (Red Hat package): до 7.0.70-41.ep7.el7
Дата выявления	15 февраля 2022 г.
Дата обновления	15 февраля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-4104	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. CVSSv3.0: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных Рекомендации по устранению: обновить программное обеспечение	8.1

MITRE: CVE-2022-23302 CVE-2022-23307 CVE-2020-9493	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. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-502: Десериализация недоверенных данных Рекомендации по устранению: обновить программное обеспечение	9.8

Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2022021518 http://access.redhat.com/errata/RHSA-2022:0524 http://access.redhat.com/errata/RHSA-2022:0527