НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20200518.1 | 18 мая 2020 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Apache Camel

Идентификатор уязвимости	MITRE: CVE-2020-11973 CVE-2020-11972
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 работой компонента Java в Apache Camel RabbitMQ.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимое ПО	Apache Camel до v3.1.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 мая 2020 г.
Дата обновления	17 мая 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.openwall.com/lists/oss-security/2020/05/14/8 https://www.openwall.com/lists/oss-security/2020/05/14/9 https://www.openwall.com/lists/oss-security/2020/05/14/10 https://camel.apache.org/security/CVE-2020-11973.html https://camel.apache.org/security/CVE-2020-11972.html https://www.cybersecurity-help.cz/vdb/SB2020051702