НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210917.24 | 17 сентября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Обход авторизации в Apache Shiro

Идентификатор уязвимости	MITRE: CVE-2021-41303
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти систему авторизации посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной обработкой входящих данных.
Категория уязвимого продукта	Универсальные библиотеки и компоненты
Уязвимый продукт	Apache Shiro: 1.0.0, 1.1.0, 1.2.0, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.3.0, 1.3.1, 1.3.2, 1.4.0, 1.4.1, 1.4.2, 1.5.0, 1.5.1, 1.5.2, 1.5.3, 1.6.0, 1.7.0, 1.7.1
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	17 сентября 2021 г.
Дата обновления	17 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
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)	Отсутствует (N)
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/SB2021091709 http://seclists.org/oss-sec/2021/q3/175