

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ
VULN-20200818.6 | 18 августа 2020 г.
Уровень опасности: КРИТИЧЕСКИЙ
Наличие обновления: ЕСТЬ

Удаленное выполнение кода в Apache Struts

Идентификатор уязвимости	MITRE: CVE-2019-0230
Идентификатор программной ошибки	CWE-94: Некорректное управление генерированием кода (Внедрение кода)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной обработкой OGNL-выражений.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	Struts v2.0.0 по v2.5.20
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	13 августа 2020 г.
Дата обновления	14 августа 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)	Не требуется (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://cwiki.apache.org/confluence/display/WW/S2-059